

netsys

Networking your world

NVF-800S

8VDSL +2 Giga Ethernet Managed 4-Band VDSL IP DSLAM

USER'S MANUAL



[Http://www.netsys.com.tw](http://www.netsys.com.tw)



Copyright

Copyright © 2011 by National Enhance Technology Corp. All rights reserved.

Trademarks

NETSYS is a trademark of National Enhance Technology Corp.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, National Enhance Technology Corp. hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETSYS reserves the right to make changes to the products described in this document without notice. NETSYS does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Maximum signal rate derived from IEEE Standard specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate. Netsys does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Make sure you follow in line with the environmental conditions to use this product.

Foreword: VDSL Solution

The 4-Band VDSL IP DSLAM networking solution delivers cost-effective, high-performance broadband access to multi-unit buildings (hotels, motels, apartment, offices and multi-tenant unit buildings) and enterprise campus environments such as manufacturing, educational campuses and medical facilities. VDSL technology dramatically extends Ethernet over existing Category 1/2/3 wiring at speeds from 5/15/25 Mbps (full duplex) and distances up to 1700/1100/600 meters(5666/3666/1999 feet). The VDSL technology delivers broadband service on the same lines as **Plain Old Telephone Service** (POTS), digital telephone and ISDN system. In addition, VDSL supports mode compatible with symmetric digital subscriber line, allowing service providers to provision VDSL to buildings where broadband services already exist.

The 4-Band VDSL solution includes 8 ports IP DSLAM as CO side, and 4-Band VDSL converter as CPE device.

The 4-Band VDSL solution delivers everything needed to quickly deploy an Ethernet-based network with the performance required to deliver high-speed Internet access at much greater distances and drive services like IP telephony and audio/video streaming. With this technology, a broad range of customers can benefit from lower operating costs and rapid deployment. The 4-Band VDSL solution provides multicast, Layer 2 quality of service (QoS), Link Aggregation (LACP) dynamic trunking group, security, GVRP, IGMP for VOD (Video on demand) and SNMP RMON management and Web-based NVF-800S network management.

The 4-Band VDSL IP DSLAM is a switch between external Internet backbone through a bridge for IP sharing and the building 110D telephone rack or telephone box. It utilizes the available telephone wire to enable high-speed Internet access to building residents.

The 4-Band IP DSLAM uses the phone line networking technology endorsed by the VDSL (Very High Data Rate DSL), and it utilizes the already existing telephone wire to deliver 5/15/25 Mbps Internet access on each RJ-45 port. This gives users a low-cost, end-to-end solution and eliminates the need to train installation teams on multiple systems.

8 Ports 5/15/25M 4-Band VDSL IP DSLAM + 2 10/100/1000M Giga Ethernet

The 4-Band VDSL IP DSLAM has 8 x 5/15/25M VDSL ports and 2 x 10/100/1000M Ethernet ports. The NVF-800S is one rack-unit (1RU) high, 10-inches deep. It is a standard Rack mounted size.

4-Band IP DSLAM deliver dedicated bandwidth per port at rates of 5/15/25 Mbps. VDSL transmissions coexist with POTS and ISDN, and can be compatible with ADSL/HomePNA traffic in the same building. The NVF-800S can be configured on a per-NVF-800S basis to support the following modes:

- 5 Mbps symmetrical rate (up to 1700 meters / 5666 feet)
- 15 Mbps symmetrical rate (up to 1100 meters / 3666 feet)
- 25 Mbps symmetrical rate (up to 600 meters / 1999 feet)

The 4-Band VDSL IP DSLAM and 4-Band VDSL Bridge provide fast and easy connectivity into building patch panels with RJ-45 connector. The 10/100/1000 Giga Ethernet ports can be used to connect servers, Ethernet. These connectivity options provide multiple price/performance options to meet building and budget requirements.

Attention:

Be sure to read this manual carefully before using this product. Especially Legal Disclaimer, Statement of Conditions and Safty Warnings.

Caution:

The NVF-800S are for **indoor** applications only. This product does not have waterproof protection. Do not use in harsh environments (Over temperature range: 0°C ~ 50°C (32°F ~ 122°F)).

The 4-Band VDSL IP DSLAM provides the important features necessary for robust networks:

Class of Service:	802.1p CoS support. Provides high-and low-priority queuing on a per-port basis.
IGMP Snooping:	By 1K IP multicast table for VOD (Video on demand) and video conference and internet games application.
Scalability:	Up to 5/15/25 Mbps symmetric performance over single-pair wiring. Fast Ether Channel port aggregation.
Security:	802.1Q Tagging-based and 802.1V protocol-based virtual local-area network (VLAN) support. Private VLAN access, assuring port security without requiring a VLAN per port, and also supports MAC filtering.
In band Management:	NVF-800S provides a console port for setup IP or other function.
Out of band Management:	NVF-800S supports remote control by Telnet and Web-based. Management easy-to-use configuration and ongoing monitoring. This software is embedded in the VDSL NVF-800S and delivers remote, intuitive management of NVF-800S and connected VDSL CPE devices through a single IP address. NVF-800S are easy-to-configure and deploy, and offer a compelling option in terms of cost, performance, scalability and services compared to traditional ATM-based xDSL solutions.
IEEE-802.1d Spanning tree:	This function is for MAC bridge to avoid port loop and link redundant.
IEEE-802.3ad port trunking:	Namely link aggregation
Port Mirroring:	This function could be mirroring and duplicate client side action as E-Mail, but need to be with mirroring AP as Session Wall or others.
Broadcast storm filtering:	This function is to avoid connecting node too much to cause broadcast storm.
TFTP protocol:	This function is for remote firmware upgrade and remote setup value backup and restore.

SNMP:	Support RFC-1493 bridge MIB; RFC-1213 MIB II; RFC-1643 Ethernet MIB and RFC-1757 RMON MIB with 1,2,3,9 groups.
Supports Interleave Setup:	To prevent the transmission against burst errors.
SNR(Signal to Noise Ratio) indicator :	This function is for checking CO and CPE both connecting quality over phone wiring.
Alarm:	In order to make sure system normal working, NVF-800S provides Fan and Temperature monitor and management, you can through WEB or Telnet to show internal temperature and Fan speed, if temperature exceeds 70°C or Fan rotation stops , the NVF-800S will send a SNMP trap to inform of Trap management server.
Hacker prevention:	To avoid hacker to enter management system through client side, the 8 ports NVF-800S will filter system IP from client side for preventing hacker attacking.
Supports multiple web browsers:	Supports multiple web browsers, i.e. IE & Firefox under Windows OS, Mozilla & Firefox under Linux OS.
Supports Interleave Setup:	To prevent the transmission against noise and data errors.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions before using the device.

- ◆ **DO NOT** open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. **ONLY** qualified service personnel can service the device. Please contact your vendor for further information.
- ◆ **Use ONLY** the dedicated power supply for your device. Connect the power cord or power adapter to the right supply voltage (110V AC in North America or 230V AC in Europe).
- ◆ **DO NOT** use the device if the power supply is damaged as it might cause electrocution. If the power supply is damaged, remove it from the power outlet. **DO NOT** attempt to repair the power supply. Contact your local vendor to order a new power supply.
- ◆ **Place** connecting cables carefully so that no one will step on them or stumble over them. **DO NOT** allow anything to rest on the power cord and do not locate the product where anyone can work on the power cord.
- ◆ **DO NOT** install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- ◆ **DO NOT** expose your device to dampness, dust or corrosive liquids.
- ◆ **DO NOT** use this product near water, for example, in a wet basement or near a swimming pool.
- ◆ **Connect ONLY** suitable accessories to the device. Make sure to connect the cables to the correct ports.
- ◆ **DO NOT** obstruct the device ventilation slots, as insufficient airflow may harm your device.
- ◆ **DO NOT** place items on the device.
- ◆ **DO NOT** use the device for outdoor applications, and make sure all the connections are indoors. There may be a remote risk of electric shock from lightning.
- ◆ **Be careful** when unplugging the power, because the transformer may be very hot.
- ◆ **Keep** the device and all its parts and accessories out of children's reach.
- ◆ **Clean** the device using a soft and dry cloth rather than liquid or atomizers. Power off the equipment before cleansing it.
- ◆ This product is **recyclable**. Dispose of it properly.

Table of Contents

Copyright	1
Foreword: VDSL Solution	2
Safety Warnings	6
Chapter 1. Unpacking Information	12
1.1 Check List	12
1.2 Package Contents	12
1.3 Product Guide	13
Chapter 2. General Description	17
2.1 Hardware Description	17
2.2 Front Panel	17
2.3 LED Indications	19
2.4 Rear Panel	20
Chapter 3. Complete Installation	21
3.1 Hardware Installation	21
3.2 Pre-Installation Requirements	21
3.3 General Rules	22
3.4 NVF-800S Connections	22
3.5 "MDI-X" Station Port Connections	22
3.6 "MDI" Port (TX) Connections	23
3.7 Basic Configuration	24
Chapter 4. Management Configuration	25
4.1 In-Band Management	25

4.1.1 Main Menu	29
4.1.1.1 Status and Counters	30
4.1.1.1.1 Port Status	31
4.1.1.1.2 Port Counters	32
4.1.1.1.3 System Information	34
4.1.1.2 Switch Static Configuration	35
4.1.1.2.1 Administration Configuration	36
4.1.1.2.1.1 Device Configuration	37
4.1.1.2.1.2 IP Configuration	38
4.1.1.2.1.3 Change Username	39
4.1.1.2.1.4 Change Password	40
4.1.1.2.2 Port/Trunk Configuration	41
4.1.1.2.3 Port Mirroring Configuration	42
4.1.1.2.4 VLAN Configuration	44
4.1.1.2.4.1 VLAN Configure	45
4.1.1.2.4.2 Create a VLAN Group	49
4.1.1.2.4.3 Edit/Delete a VLAN Group	50
4.1.1.2.5 Priority Configuration	51
4.1.1.2.6 MAC Address Configuration	52
4.1.1.2.6.1 Static MAC Address	53
4.1.1.2.6.1.1 Add Static MAC Address	54
4.1.1.2.6.2 Filtering MAC Address	55
4.1.1.2.6.2.1 Add Filtering MAC Address	56
4.1.1.2.7 Misc Configuration	57

4.1.1.2.7.1 Port Security	58
4.1.1.2.7.2 MAC Age Interval.....	59
4.1.1.2.7.3 Broadcast Storm Filtering.....	60
4.1.1.2.7.4 Max Bridge Transmit Delay Bound.....	61
4.1.1.3 Protocol Related Configuration	62
4.1.1.3.1 STP	63
4.1.1.3.1.1 STP Enable.....	64
4.1.1.3.1.2 System Configuration.....	65
4.1.1.3.1.3 Perport Configuration.....	66
4.1.1.3.2 SNMP	67
4.1.1.3.2.1 System Options.....	68
4.1.1.3.2.2 Community Strings.....	69
4.1.1.3.2.2.1 Add SNMP Community	70
4.1.1.3.2.3 Trap Managers.....	71
4.1.1.3.2.3.1 Add SNMP Trap Manager.....	72
4.1.1.3.3 GVRP	73
4.1.1.3.4 LACP	74
4.1.1.3.4.1 Aggregator Setting.....	75
4.1.1.3.4.2 State Activity.....	76
4.1.1.3.4.3 LACP Status	77
4.1.1.4 Temperature and Fan Monitor.....	78
4.1.1.5 Reboot Switch	79
4.1.1.5.1 Default	80
4.1.1.5.2 Reboot Switch.....	82

4.1.1.6 Command Line	83
4.1.1.7 Logout	84
4.2 Remote Network Management	85
4.2.1 IP Setting	85
4.2.2 Web Management Function.....	86
4.2.2.1 Web Management Home Overview	87
4.2.2.2 Port Status.....	88
4.2.2.3 Port Statistics	90
4.2.2.4 Administrator	91
4.2.2.4.1 IP Address	92
4.2.2.4.2 NVF-800S Settings	93
4.2.2.4.2.1 Basic.....	93
4.2.2.4.2.2 Advanced.....	94
4.2.2.4.3 Console Port Information	97
4.2.2.4.4 VDSL Speed Control and port Enable/Disable	97
4.2.2.4.5 Link Aggregation	99
4.2.2.4.5.1 Aggregator setting.....	99
4.2.2.4.5.2 Aggregator Information	101
4.2.2.4.5.3 State Activity	102
4.2.2.4.6 Filter Database	103
4.2.2.4.6.1 IGMP Snooping	103
4.2.2.4.6.2 Static MAC Address.....	105
4.2.2.4.6.3 Port Security	106
4.2.2.4.6.4 MAC Filtering.....	107

4.2.2.4.7 VLAN Configuration	108
4.2.2.4.7.1 Basic.....	110
4.2.2.4.7.2 Port VID	111
4.2.2.4.8 Spanning Tree Protocol	113
4.2.2.4.9 Port Sniffer.....	116
4.2.2.4.10 SNMP	117
4.2.2.4.11 Interleave.....	119
4.2.2.4.12 SNR.....	122
4.2.2.4.13 Security Manager.....	123
4.2.2.4.14 TFTP Update Firmware.....	123
4.2.2.4.15 Configuration Backup.....	124
4.2.2.4.16 Reset System	125
4.2.2.4.17 Reboot	125
Chapter 5: Applications	126
Appendix A: Cable Requirements.....	130
Appendix B: Troubleshooting	134
Appendix C: VDSL Spectrum	139
Appendix D: 4 Band VDSL Electrical Characteristics	140
Appendix E: Examples of VLAN Setting.....	141
Appendix F: Compliance and Safety Information	152
Warranty	155
Chinese SJ/T 11364-2006.....	156

Chapter 1. Unpacking Information

1.1 Check List

Carefully unpack the package and check its contents against the checklist.

1.2 Package Contents

1. 1 x NVF-800S 4-Band VDSL IP DSLAM
(2 x 10/100/1000 Giga Ethernet ports and 8 x 5/15/25Mbps VDSL ports)
2. 1 x User's manual CD
3. 1 x AC Power Cord
4. 2 x Rack Mounting Brackets
5. 4 x Screws
6. 4 x Plastic feet(Pre-installed on the bottom)

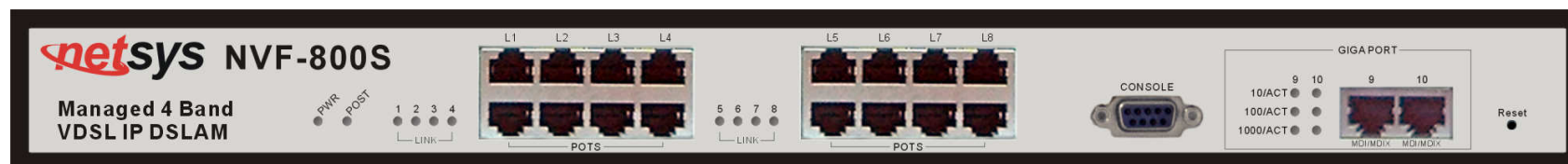
Note:

Please inform your dealer immediately for any missing or damaged parts.

If possible, retain the carton including the original packing materials.

Use them to repack the unit in case there is a need to return for repair.

1.3 Product Guide



Product Name: 2ports 10/100/1000Mbps Giga Ethernet plus 8ports 4-Band VDSL with SNMP Management IP DSLAM

Application : *Hotel, Campus, Hospital, Telecom, Industrial etc.*

Key Features:

- ◆ Supports 5M/15M/25Mbps per port symmetrical bandwidth over phone wiring with long driver capable 1.7/1.1/0.6km(5666/3666/1999 feet) with auto speed and fix speed selectable through web management.
- ◆ Provides 2 x 10/100/1000Mbps Ethernet RJ-45 Ports with Auto MDI/MDIX
- ◆ Supports quality of phone wiring detected with SNR(Signal to Noise Ratio) indications
- ◆ Supports GARP/GVRP IEEE-802.1p/q VLAN with 256 groups static VID or 4094 groups dynamic VID
- ◆ Supports IEEE 802.1q tagging VLAN
- ◆ Supports IEEE 802.1v protocol VLAN
- ◆ Support port base VLAN
- ◆ Supports QOS IEEE-802.1p
- ◆ Supports 1K Multicast IP table/IGMP v2
- ◆ Supports LACP IEEE-802.3ad Port Trunking(Link aggregation)
- ◆ Supports IEEE 802.1d Spanning trees for MAC bridge with redundant link
- ◆ Supports port Mirroring (Sniffer)
- ◆ Support Broadcast Storm filtering

- ◆ Ethernet transport with POTS / ISDN traffic over single copper wire pair
- ◆ Spectral compatibility with XDSL, ISDN(2B1Q/4B3T), HomePNA
- ◆ Supports port security with MAC address filtering.
- ◆ Supports Web Base and Telnet for remote management
- ◆ Supports system POST(Power On Self testing) LED
- ◆ Supports SNMP v1 RFC-1493 Bridge MIBs
 - RFC-1643 Ethernet MIB
 - RFC-1213 MIB II
 - Netsys Enterprise MIB(Fan and Temperature management)
- ◆ Supports RMON groups 1(Statistics), 2(Alarm), 3(Event), 9(History)
- ◆ Cascading up to 8 Units along with Giga NVF-800S
- ◆ Supports TFTP/Xmodem for firmware upgrade
- ◆ Supports In-Band/Out-of-Band Management
- ◆ Supports Fan & Temperature Monitor & management
- ◆ Supports Interleave Setup
- ◆ Surge protected for VDSL ports
- ◆ Splitter on board

Product Specifications

- Compliant with IEEE 802.3 & 802.3u & 802.3ab Ethernet Standards
- Compliant with ETSI, ITU & ANSI standards
- 10/100/1000Mbps Ethernet ports: 2 x RJ-45 with auto crossover
- POTS/ISDN Splitter port: 8 x RJ-45
- VDSL port: 8 x RJ-45
- MAC address table: 8K Entries
- Switching method: Store-and-forward
- Flow control method by IEEE802.3x for Full Duplex & Back Pressure for Half Duplex
- Compliant with GARP/GVRP IEEE 802.1p/q port-base VLAN with 256 groups static VID or 4094 dynamic VID
- Compliant with IEEE 802.1v protocol-base VLAN classification
- Compliant with IEEE 802.1d Spanning trees
- Multicast IP table: 1K groups
- Compliant with IEEE 802.1p QOS by class of service with 2-level priority queuing
- Compliant with LACP IEEE 802.3ad Trunking
- RS-232 console port: DB-9Pin Female / 9600bps
- SNMP v1 RFC-1493 Bridge MIBs
 - RFC-1643 Ethernet MIB
 - RFC-1213 MIB II
 - Enterprise MIBs
 - RMON groups 1(Statistics), 2(Alarm), 3(Event), 9(History)
- Port security by MAC address filtering

- LED indication: Power good and POST LED
Link/Active/Speed Status for Ethernet port.
Link for VDSL port.
- VDSL Frequency Spectrum: Transmitter: 900kHz ~ 3.9 MHz
Receiver: 4MHz ~ 7.9 MHz
- POTS/ISDN Pass Filter Spectrum: 0 ~ 630 kHz
- Internal Switching Power Adapter Input: AC 85-265 volts/50-60Hz/1A.
- Dimensions: 435 x 255 x 44 mm
- Weight: about 4kgs
- Power Consumption: 18.7W
- Operating Temperature: 0°C ~ 50°C (32°F ~ 122°F)
- Storage Temperature: -20°C ~ 70°C (-4°F ~ 158°F)
- Humidity: 10% ~ 90% non-condensing
- Safety: FCC, CE Mark
- RoHS compliant

Chapter 2. General Description

2.1 Hardware Description

This section describes the important parts of the NVF-800S. It features the front and rear panel drawings showing the LED, connectors and NVF-800S.

2.2 Front Panel

The following figure shows the front panel.(Figure 2.1)

1. VDSL Ports(L1~L8)
2. POTS Ports(L1~L8)
3. Console(Baud rate: 9600 bps)
4. RJ-45 Gigabit Port(port 9-10)
5. Reset button

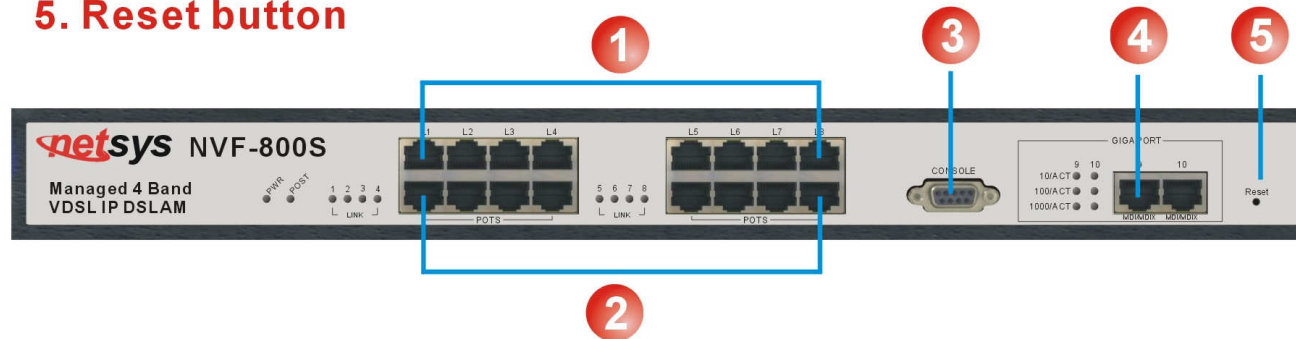


Figure 2.1 Front Panel description

Front panel description:

- “PWR”: Power LED light
- “POST”: Power On Self Testing LED light
- 2 X 10/100/1000 Mbps auto-negotiation Giga Ethernet ports
- 8 X 5/15/25 Mbps VDSL ports.
- 8 X POTS/ISDN Splitter ports.
- RS-232 Console port
- Reset Button

Tip:

NVF-800S has **Splitter embedded** between each VDSL and POTS. It permits you to deliver broadband service on the same lines as Plain Old Telephone Service (POTS), PBX, ISDN traffic and VDSL Signal.

Several LED indicators for monitoring the device itself, and the network status. At a quick glance of the front panel, the user would be able to determine if the product is receiving power, if it is monitoring another IP DSLAM or if a problem exists on the network.

2.3 LED Indications

The following describes the function of each LED indicator. (Table 2-1)

Table 2-1 LED Indicators Description and Operation

LEDs	Color	Status	Descriptions
PWR (Power LED)	Green	Steady	This LED light is located at the left side on the front panel. It will light up (ON) to show that the product is receiving power. Conversely, no light (LED OFF) means the product is not receiving power.
POST	Green	Steady	POST(Power On Self Testing)POST Led will light to show system is booting now. When system is ready the led will light off.
VDSL Link	Green	Steady	Each RJ11 station port on the VDSL is assigned an LED light for “Good Linkage”. Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage.
10 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for “10M Good Linkage”. Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.
100 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for “100M Good Linkage”. Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.
1000 LINK/ACT	Green	Steady Blinking	Each RJ45 station port on the Ethernet is assigned an LED light for “1000M Good Linkage”. Each LED is normally OFF after the power on operation, but will light up steadily to show good linkage. And Flashing to show data transmission.

2.4 Rear Panel

The following figure shows the rear panel.(Figure 2.2)

1. FAN
2. AC Power(100~240V)

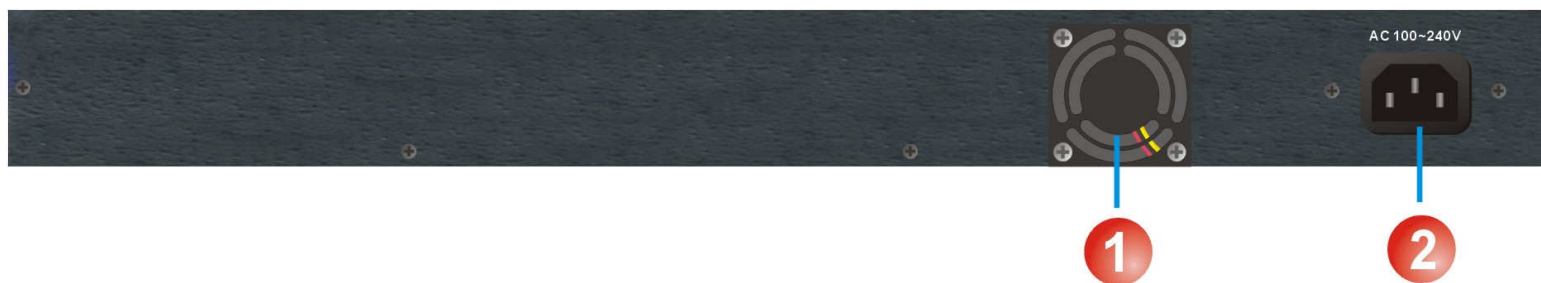


Figure 2.2 Rear Panel description

Note:

AC Power Socket: The power cord should be plug into this socket. The AC Socket accepts AC power 100 to 240 voltage.

Chapter 3. Complete Installation

3.1 Hardware Installation

This chapter describes how to install the NVF-800S. To established network connection. You may install the NVF-800S on any level surface (table, shelf, 19 inch rack or wall mounting). However, please take note of the following minimum site requirements before you begin.

3.2 Pre-Installation Requirements

Before you start actual hardware installation, make sure you can provide the right operating environment, including power requirements, sufficient physical space, and proximity to other network devices that are to be connected. Verify the following installation requirement:

- Power requirements: AC 85V to 265 V at 50 to 60 Hz.

Tip:

The Switching power supply automatically adjusts to the input voltage level.

- The NVF-800S should be located in a **cool dry place**, with at least **10cm/4in** of space at the front and back for ventilation.
- Place the NVF-800S away from **direct sunlight**, **heat sources**, or areas with a high amount of electromagnetic interference.
- Check if network cables and connectors needed for installation are available.
- Do Not install phone lines strapped together with AC power lines, or telephone office line with voice signal.
- **Avoid installing this device with radio amplifying station nearby or transformer station nearby.**
- **Please note NVF-800S internal splitter, can pass through voice spectrum is 0KHz ~ 630KHz.**

3.3 General Rules

Before making any connections to the NVF-800S, note the following rules:

- **Ethernet Port (RJ-45)**

All network connections to the NVF-800S Ethernet port must be made using Category 5 UTP for 100Mbps and Category 3, 4 UTP for 10Mbps. No more than 100 meters (about 333 feet) of cabling may be use between NVF-800S or with HUB or an end node.

- **VDSL Port (RJ-11)**

All home network connections to the VDSL Port must use **18 ~ 26** gauge with twisted pair phone wiring.

- We **do not** recommend **using 28 Gauge** or above phone line.

3.4 NVF-800S Connections

The NVF-800S has 2 x 10/100/1000Mbps Ethernet ports which support connection to 10/100/1000Mbps Giga Ethernet. The NVF-800S also supports full or half-duplex operation and the transmission mode is auto-negotiation. Therefore, the devices attached to these ports must support auto-negotiation unless they will always operate at half duplex. If transmissions must run at full duplex, but the attached device does not support auto-negotiation then one should upgrade this device to a newer version that supports auto-negotiation and auto-crossover (MDI/MDIX).

3.5 “MDI-X” Station Port Connections

1. Connect the port “9 or 10” on the NVF-800S to any device that uses a standard network interface such as a Cable bridge, ADSL bridge, Ethernet Switch, workstation, server or to a network interconnection device such as a bridge or bridge, but depends on the port type implemented.
2. Prepare the network devices one wish to connect. Make sure one have installed suitable VDSL Bridge before

making a connection to any of the NVF-800S (L1-L8) station ports. Prepare also **18 ~ 26 gauge** twisted pair phone wiring with RJ-45 plugs at both ends.

3. Connect one end of the cable to the RJ-45 port of the Home Access network adapter and the other end to any available (1 ~ 8) station port on the VDSL. Every port supports 5/15/25Mbps connections. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Caution:

Do not plug a RJ-11 phone jack connector into the Ethernet port (RJ-45 port). This may damage the HPNA. Instead, use only twisted-pair cables with RJ-45 connectors that conform the FCC standards.

Notes:

1. Be sure each twisted-pair cable (RJ-45) is not over by 100 meters (328 feet).
2. RJ-11 port use 18 ~ 26 gauge phone wiring, 28 gauge or above is not recommended.
3. We advise using Category 5 cable for Cable Modem or router connections or to attach to any high bandwidth device to avoid any confusion or inconvenience.

3.6 “MDI” Port (TX) Connections

Prepare straight through shielded or unshielded twisted pair cables with RJ-45 plugs on both ends. Use 100Ω Category 5 cable for connections. Connect one end of the cable to port “9 or 10” of the NVF-800S and the other end to a standard RJ-45 station port on cable bridge, ADSL bridge, wireless bridge, etc. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Note:

Make sure the length of twisted-pair cable is not over by 100 meters (328 feet).

3.7 Basic Configuration

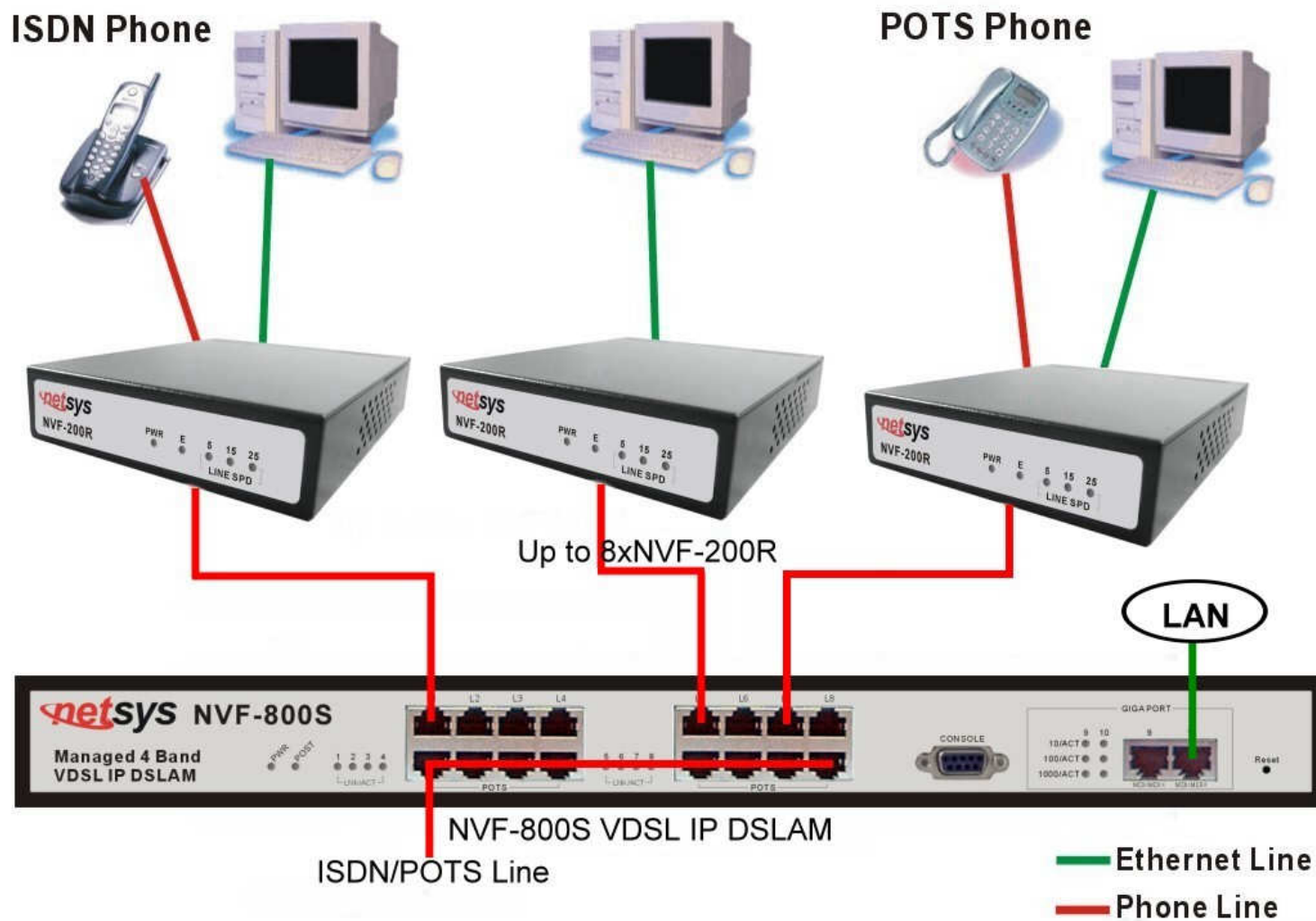


Figure 3.1 NVF-800S Basic Application Diagram

Chapter 4. Management Configuration

4.1 In-Band Management

Console port (RS-232) Configuration

Configure the unit with the local serial console port, if one of the RJ11 port is not in use, you can disable it by connecting a notebook computer to the RS-232 port, then boot with windows OS system and launch “Hyperterminal” program into terminal window. Setup steps are as follow: (Figure 4.1)

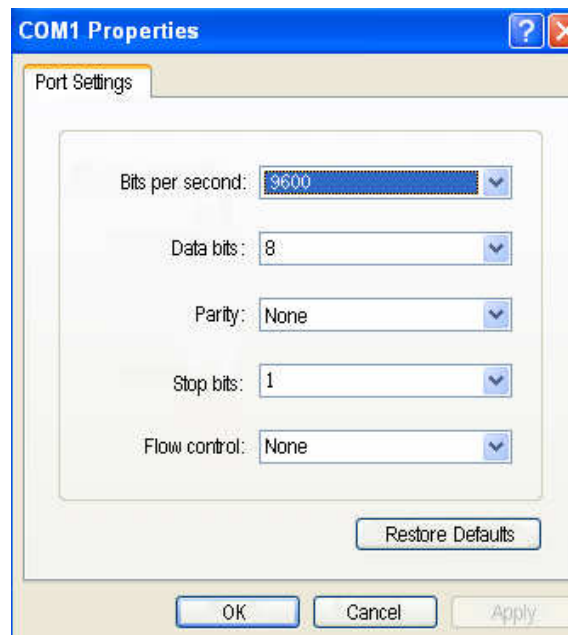


Figure 4.1 COM1 Properties

1. Set “**Bits per second**” at **9600** to the content window.
2. Set “**Flow control**” at **None**

3. Connects PC with the NVF-800S, you will find login manual window on the screen then enter
Login name : "**admin**" ; password : "**123**". (Figure 4.2)

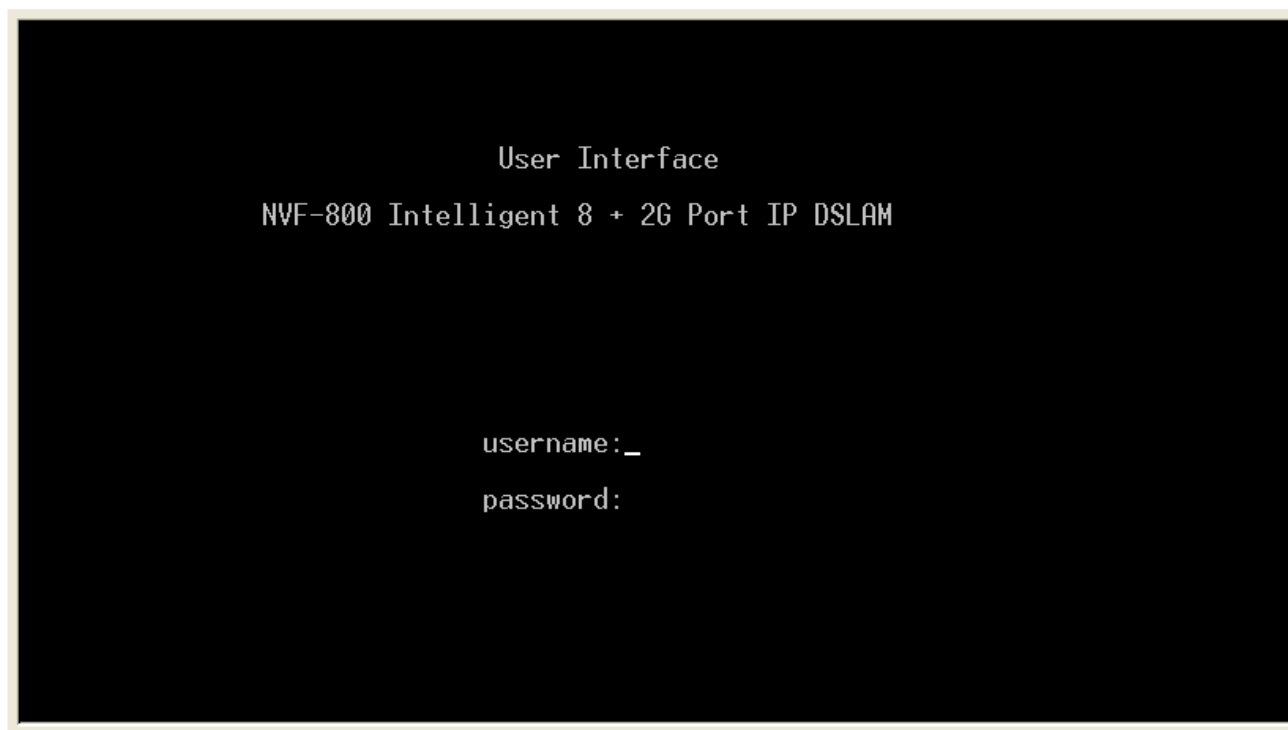


Figure 4.2 User Interface

4. This is the main menu screen: (Figure 4.3)



Figure 4.3 Main Menu

Operation Button:

Tab=Next Item;

Backspace=Previous Item;

Enter=Select Item

Change the IP Configuration, enter the IP configuration page and follow these steps: (Figure 4.4)

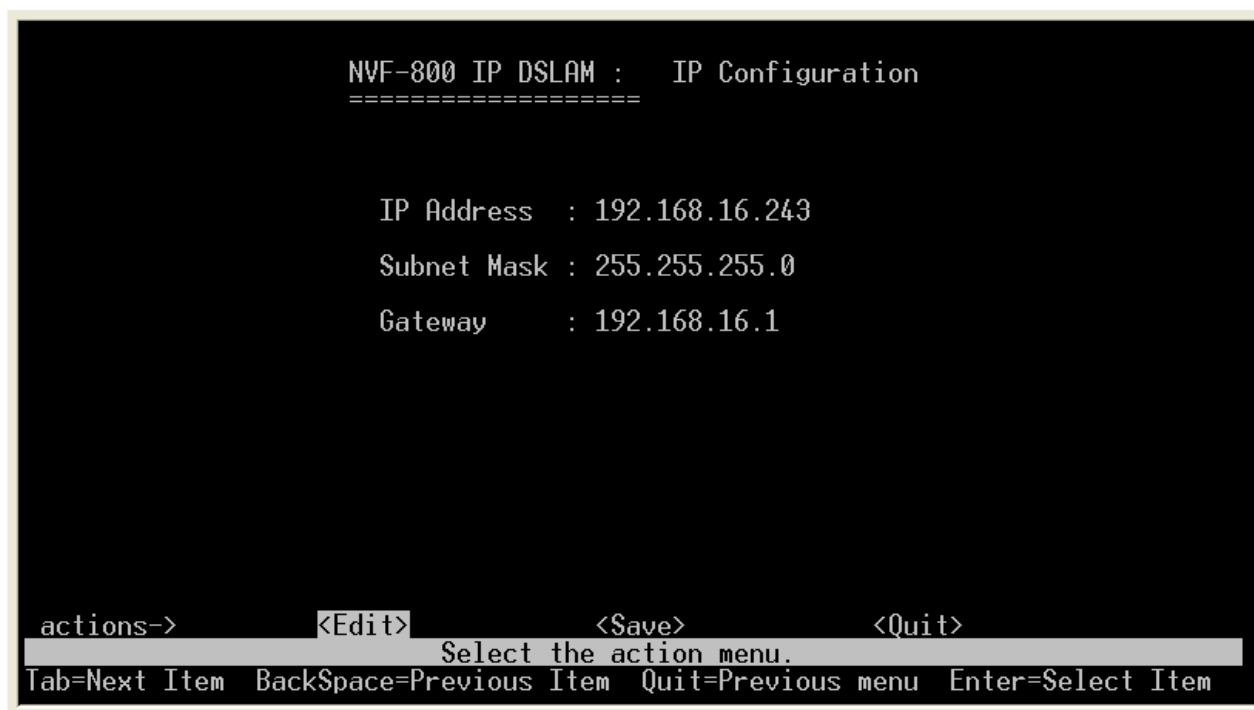


Figure 4.4 IP Configuraiton

1. Choose **Edit** item to Change IP address, Subnet Mask and Gateway.
2. Use **CTRL+A** button to back actions choice.
3. Choose **Save** item to save change and back to System Configuration page.
4. Choose **Previous Menu** item to quit System Configuration page.
5. Choose **Main Menu** item to quit NVF-800S Configuration page and back to Main Manual.
6. Choose **Reboot NVF-800S** item.
7. Choose **Restart** item to reboot your NVF-800S.

4.1.1 Main Menu

There is an easy Setup for end users at the setup of NVF-800S with [Status and Counters](#), [Switch Static Configuration](#), [Protocol Related Configuration](#), [Temperature & Fan Monitor](#), [Reboot Switch](#), [Command Line](#), [Logout](#) for more detail configurations. (Figure 4.5)

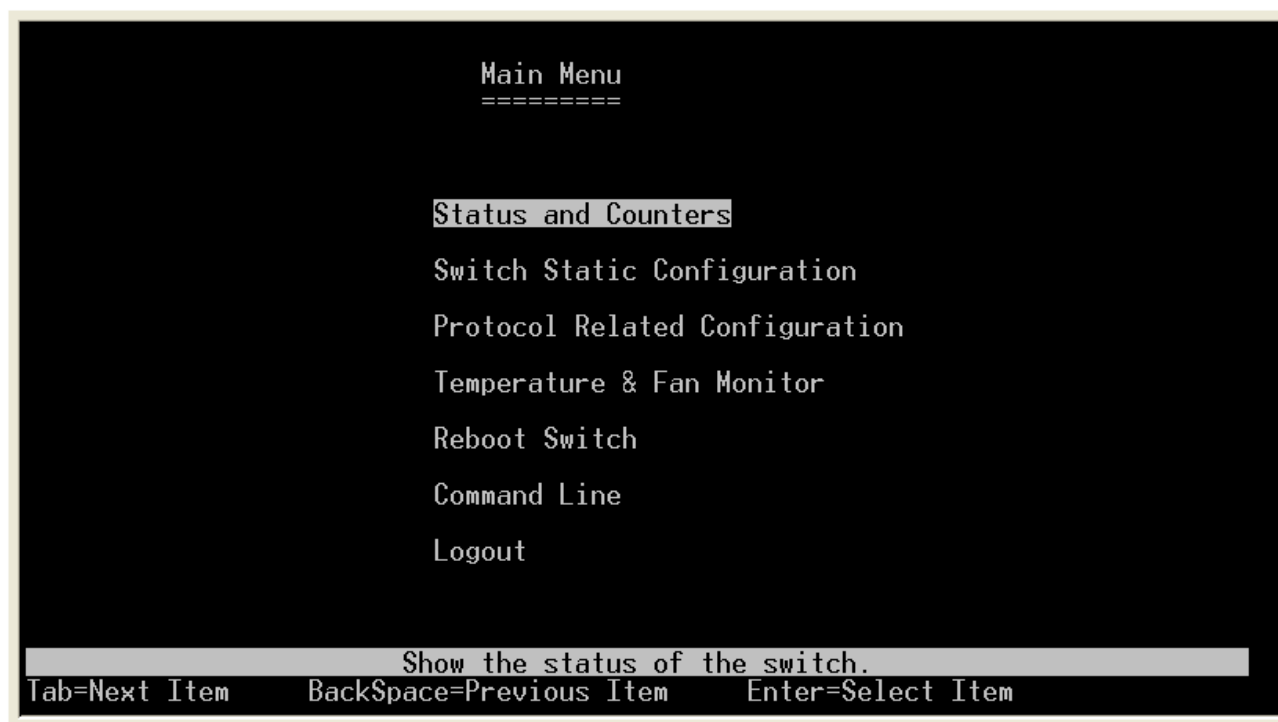


Figure 4.5 Main Menu introduction

4.1.1.1 Status and Counters

Select the "Status and Counters". The menu below includes the sub-menus of **Port Status**, **Port Counters**, **System Information** and **Main Menu**.(Figure 4.6)

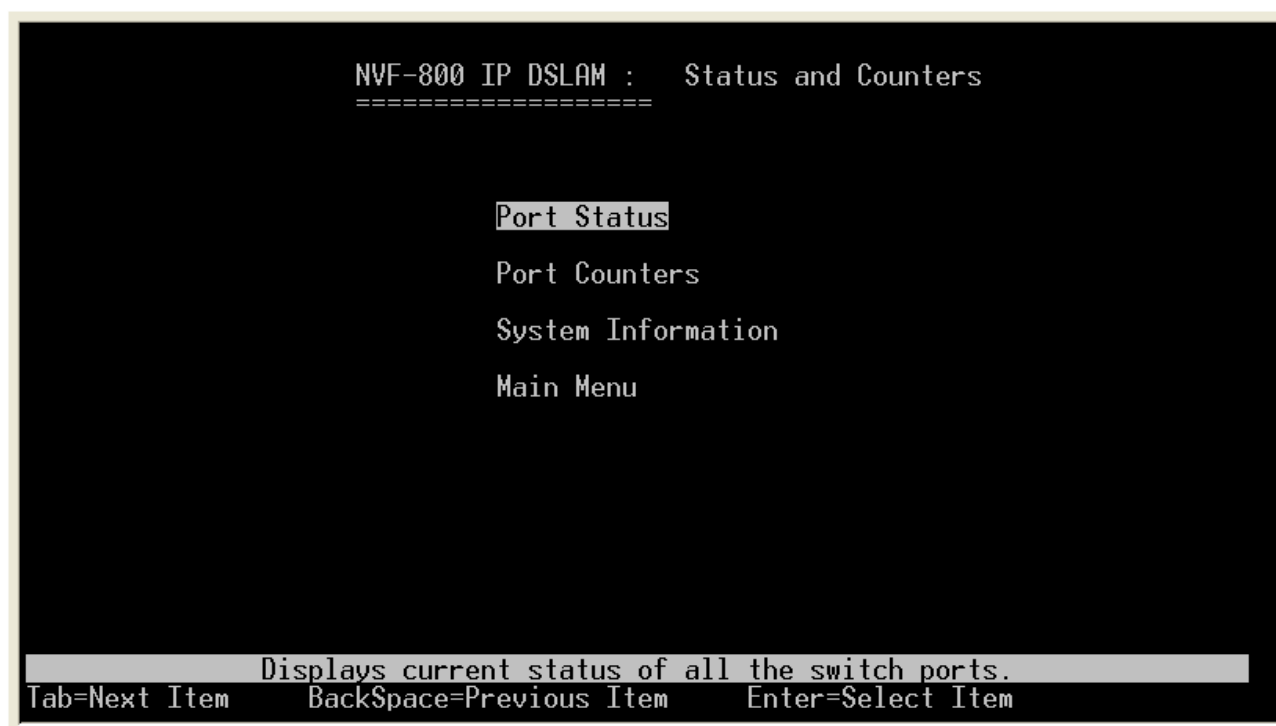
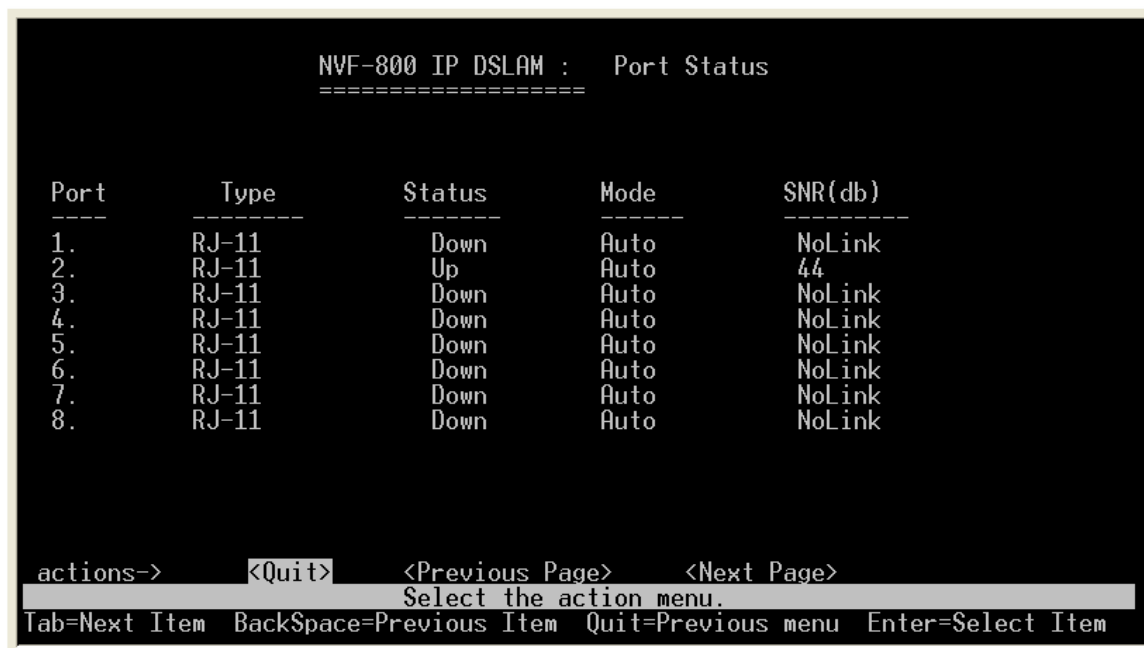


Figure 4.6 Status and Counters

4.1.1.1.1 Port Status

Displays the current status of all switch ports. (Figure 4.7)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
Type:	Shows the media type of the port's device.
Status:	Shows the condition of the port if it is up or down.
Mode:	Shows at what mode is the port set. It can either be Auto, 5M, 15M or 25Mbps.
SNR(dB):	Shows if the NVF-800S VDSL IP DSLAM is link or not and the value of SNR in dB.



NVF-800 IP DSLAM : Port Status				
Port	Type	Status	Mode	SNR(db)
1.	RJ-11	Down	Auto	NoLink
2.	RJ-11	Up	Auto	44
3.	RJ-11	Down	Auto	NoLink
4.	RJ-11	Down	Auto	NoLink
5.	RJ-11	Down	Auto	NoLink
6.	RJ-11	Down	Auto	NoLink
7.	RJ-11	Down	Auto	NoLink
8.	RJ-11	Down	Auto	NoLink

actions-> <Quit> <Previous Page> <Next Page>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

Figure 4.7 Port Status

4.1.1.1.2 Port Counters

Displays a summary of network activity. (Figure 4.8)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
TxGoodPkt and RxGoodPkt:	Shows the values of good packets transmitted and received.
TxBadPkt and RxBadPkt:	Shows the values of bad packets transmitted and received.
TxAbort:	Shows the values of the aborted packets being transmitted.
Collision:	Shows the values of packets collisions.
DropPkt:	Shows the values of packet being drop.

NVF-800 IP DSLAM : Port Counters							
=====							
Port	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1.	0	0	0	0	0	0	0
2.	39	0	0	0	0	0	0
3.	0	0	0	0	0	0	0
4.	0	0	0	0	0	0	0
5.	0	0	0	0	0	0	0
6.	0	0	0	0	0	0	0
7.	0	0	0	0	0	0	0
8.	0	0	0	0	0	0	0
actions-> <Quit> <Reset All> <Previous Page> <Next Page>							
Configure the action menu.							
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item							

Figure 4.8 Port Counters

Tip:

Packet Collision: In a network, when two or more stations attempt to transmit a packet across the network at the same time, a packet collision occurs. This is not uncommon in a shared medium such as an Ethernet that has many computers in the same network segment. When a packet collision occurs, the packets are either discarded or sent back to their originating stations and then retransmitted in a timed sequence to avoid further collision. Packet collisions can result in the loss of packet integrity or can impede the performance of a network.

4.1.1.1.3 System Information

Display the switch system. (Figure 4.9)

Item	Description
System Description:	Shows the full description of NVF-800S VDSL IP DSLAM
MAC Address:	Shows the unique MAC address of the device.
Firmware version:	Shows the firmware version being used by the device.
Hardware version:	Shows the hardware version being used by the device.
Default configuration value version:	Shows the version of the default configuration being used.

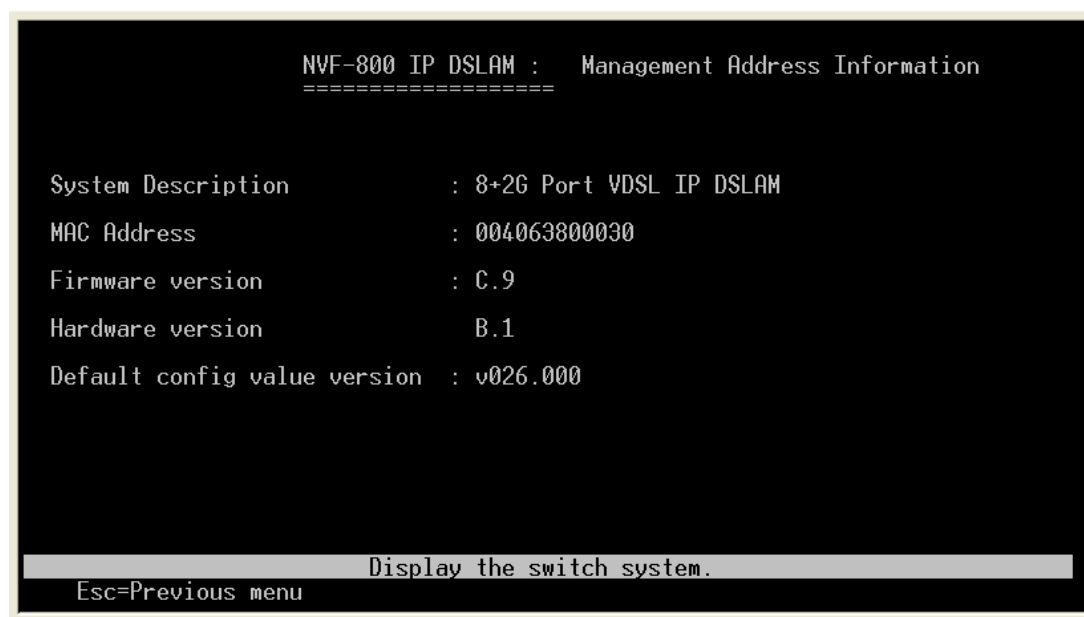


Figure 4.9 Management Address Information

4.1.1.2 Switch Static Configuration

Select the "Switch Static Configuration". The menu below includes the sub-menus of Administration, Port/Trunk, Port Mirroring, VLAN, Priority, Mac Address, Misc and Main Menu. (Figure 4.10)



Figure 4.10 Switch Configuration

4.1.1.2.1 Administration Configuration

Select the "Administration Configuration". The menu below includes the sub-menus of **Device Information**, **IP configuration**, **Change Username** and **Change Password**. Please configure the Administration items as follows. (Figure 4.11)



Figure 4.11 Administration Configuration

4.1.1.2.1.1 Device Configuration

Configure the device information, you can edit and create your own name. (Figure 4.12)

Item	Description
Device Name:	Shows the whole device name.
Device Content:	Shows the content of the device.
Device Location:	Shows the location of the device.
Device Description:	Shows the description of the device.

```

NVF-800 IP DSLAM : Device Information
=====

Device Name : VDSL IP DSLAM
Device Content : VDSL PORTS
Device Location : EARTH
Device Description : 8+2G Port VDSL IP DSLAM

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 4.12 Device Information

4.1.1.2.1.2 IP Configuration

Configure the IP(Internet Protocol) information. (Figure 4.13)

Item	Description
IP Address:	Shows the IP address of the device.
Subnet Mask:	Shows the subnet mask of the device.
Gateway:	Shows the gateway of the device.

```

NVF-800 IP DSLAM :  IP Configuration
=====

IP Address  : 192.168.16.242
Subnet Mask : 255.255.255.0
Gateway    : 192.168.16.1

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item

```

Figure 4.13 IP Configuration

4.1.1.2.1.3 Change Username

Item	Description
Username:	Shows and configure the current username.

(Figure 4.14)



Figure 4.14 User Name Configuration

4.1.1.2.1.4 Change Password

Configure the password, type the numbers will be masked. (Figure 4.15)

Item	Description
Old Password:	Type the old password.
New Password:	Type the new password.
Enter again:	Type the new password again.



Figure 4.15 Password Configuration

4.1.1.2.2 Port/Trunk Configuration

Display or change port/trunk configuration. (Figure 4.16)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
Type:	Shows the media type of the port's device.
Enabled:	Shows and configure if the port is enabled or not.
Auto Negotiate:	Shows and configure if the port can either auto negotiate or not.
Speed/Duplex Config:	Shows and configure the speed of each port if it is Auto/5M/15M/25Mbps.
Flow Control:	Shows if the flow control on each port is either active or not.
Group:	Shows the group trunking of each port if it is None/trk1/trk2/trk3/trk4.



NVF-800 IP DSLAM : Port Configuration						
=====						
Port	Type	Enabled	Auto Negotiate	Speed/Duplex Config	Flow Control	Group

1.	RJ-11	Yes	Enabled	Auto	On	
2.	RJ-11	Yes	Enabled	Auto	On	
3.	RJ-11	Yes	Enabled	Auto	On	
4.	RJ-11	Yes	Enabled	Auto	On	
5.	RJ-11	Yes	Enabled	Auto	On	
6.	RJ-11	Yes	Enabled	Auto	On	
7.	RJ-11	Yes	Enabled	Auto	On	
8.	RJ-11	Yes	Enabled	Auto	On	
actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>						
Select the Action menu.						
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item						

Figure 4.16 Port Configuration

4.1.1.2.3 Port Mirroring Configuration

Display or change port mirror configuration. (Figure 4.17)

Item	Description
Monitoring Enable:	NO

Default monitoring enable is NO.

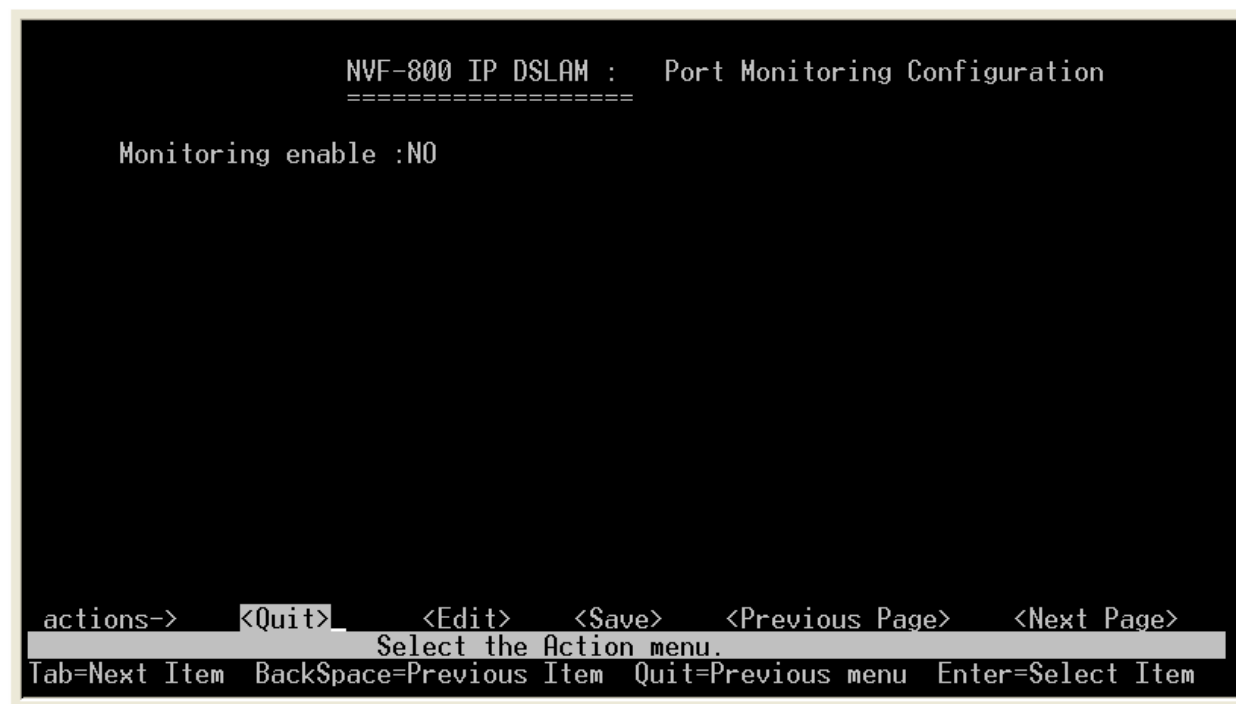


Figure 4.17 Port Monitoring Configuration(Disable)

Tip:

This function can special monitor client side as duplicate mail, Http.....etc, but need to be used with the application software(i.e. sniffer software).

Item	Description
Monitoring Enable: YES	
Monitoring Port:	Shows the monitoring port selection from port 1 to 10.
Action:	Show the action of the monitoring if it is Tx/Rx/Both.

(Figure 4.18)

```

NVF-800 IP DSLAM :  Port Monitoring Configuration
=====

Monitoring enable :YES

Monitoring Port :1
Monitored Port :

  Port      Type      Action
-----
  1.        10
  2.        10
  3.        10
  4.        10
  5.        10
  6.        10
  7.        10
  8.        10

actions->  <Quit>    <Edit>    <Save>    <Previous Page>    <Next Page>
          Edit the monitor configuration.
Tab=Next Item  BackSpace=Previous Item  Space=Toggle  Ctrl+A=Action menu

```

Figure 4.18 Port Monitoring Configuration(Enable)

4.1.1.2.4 VLAN Configuration

Select the "VLAN Configuration". The menu below includes the sub-menus of **VLAN Configure**, **Create a VLAN Group**, **Edit/Delete a VLAN Group**. Display or change VLAN (Virtual Local Area Network) configuration. ([Figure 4.19](#))

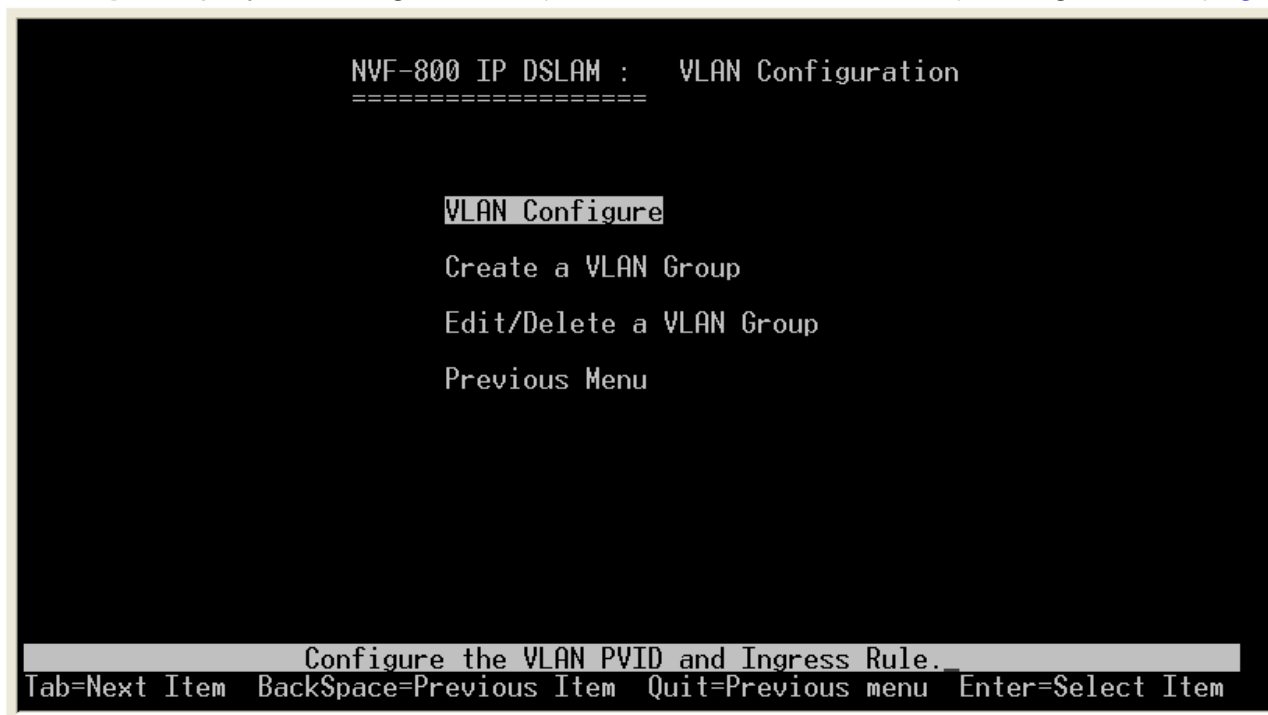


Figure 4.19 VLAN Configure

4.1.1.2.4.1 VLAN Configure

Configure the VLAN PVID and Ingress Rule.

Item	Description
VLAN Mode:	User can choose from 4 VLAN modes, respectively, 802.1Q, 802.1Q with GVRP, Port Based and Disable. Default VLAN mode is disabled.

VLAN Mode: **Disabled** (Figure 4.20)

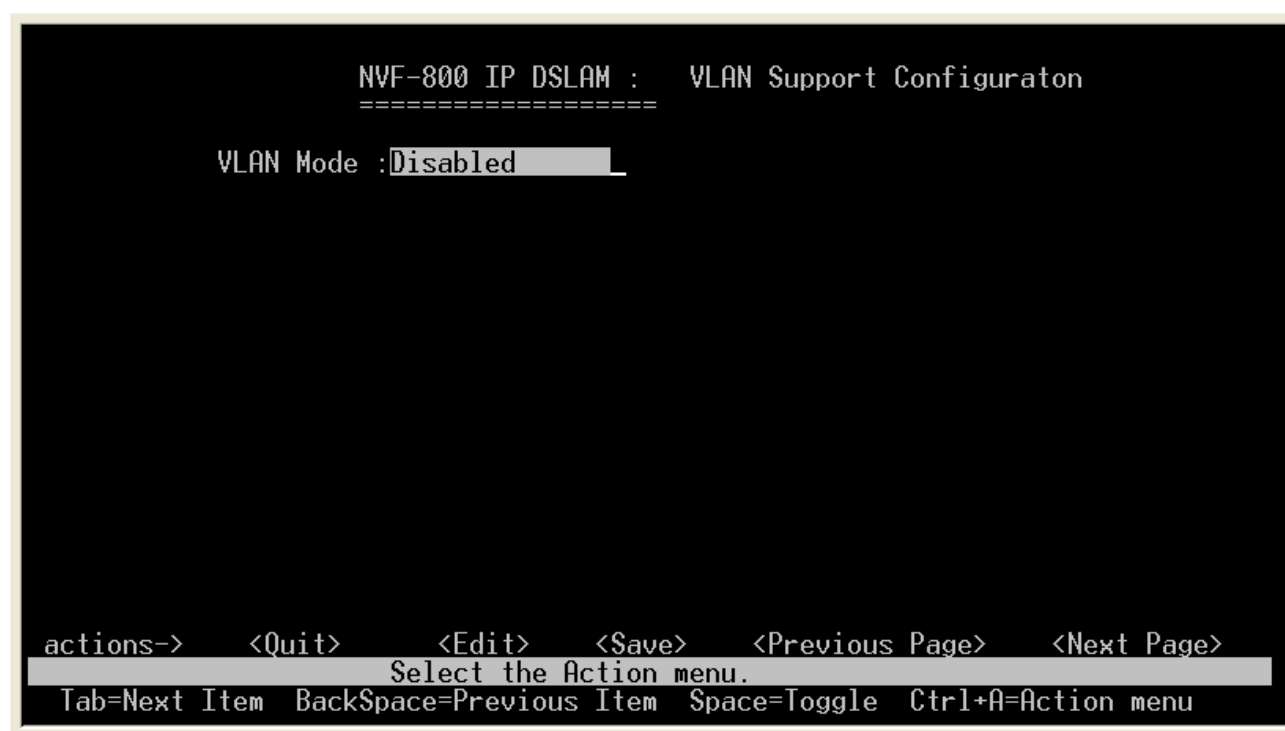
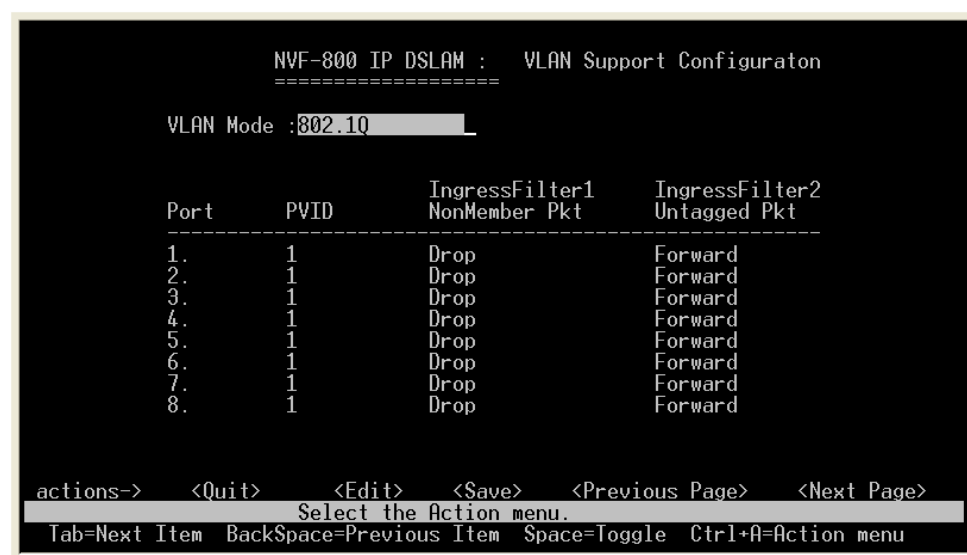


Figure 4.20 VLAN Mode: Disable

VLAN Mode: 802.1Q (Figure 4.21)

Item	Description
Port:	Shows the port of NVF-800S VDSL IP DSLAM.
PVID:	Shows the PVID value. Valid range is from 1 to 4094.
IngressFilter1 NonMember Pkt:	Shows the packet being forward only packets with VID matching this port's configured VID
IngressFilter2 Untagged Pkt:	Shows the packet being drop Untagged Frame



NVF-800 IP DSLAM : VLAN Support Configuraton			
=====			
VLAN Mode :802.1Q			
Port	PVID	IngressFilter1 NonMember Pkt	IngressFilter2 Untagged Pkt
1.	1	Drop	Forward
2.	1	Drop	Forward
3.	1	Drop	Forward
4.	1	Drop	Forward
5.	1	Drop	Forward
6.	1	Drop	Forward
7.	1	Drop	Forward
8.	1	Drop	Forward
actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>			
Select the Action menu.			
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu			

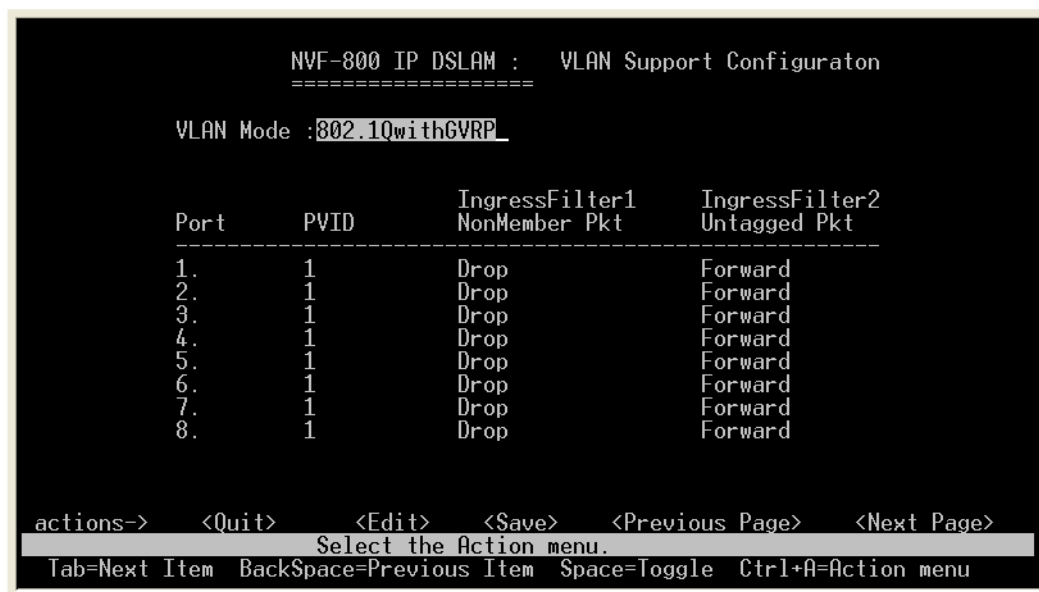
Figure 4.21 VLAN Mode: 802.1Q

Tip:

PVID: Sets the Port VLAN ID that will be assigned to untagged traffic on a given port. For example, if port 1's Default PVID is 100, all untagged packets on port 1 will belong to VLAN 100. The default setting for all ports is **VID 1**. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Only one untagged VLAN is allowed per port.

VLAN Mode: 802.1Q with GVRP(Figure 4.22)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
PVID:	Shows the PVID value. Valid range is from 1 to 4094.
IngressFilter1 NonMember Pkt:	Shows the packet being forward only packets with VID matching this port's configured VID.
IngressFilter2 Untagged Pkt:	Shows the packet being drop Untagged Frame.



```

NVF-800 IP DSLAM :  VLAN Support Configuraton
=====
VLAN Mode :802.1QwithGVRP_

Port      PVID      IngressFilter1      IngressFilter2
          PVID      NonMember Pkt      Untagged Pkt
-----
1.         1         Drop               Forward
2.         1         Drop               Forward
3.         1         Drop               Forward
4.         1         Drop               Forward
5.         1         Drop               Forward
6.         1         Drop               Forward
7.         1         Drop               Forward
8.         1         Drop               Forward

actions->  <Quit>    <Edit>    <Save>    <Previous Page>  <Next Page>
          Select the Action menu.
          Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

```

Figure 4.22 VLAN Mode: 802.1Q with GVRP

Tip:

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol): GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch, the switch will automatically add that device to the existing VLAN.

VLAN Mode: **PortBased**(Figure 4.23)

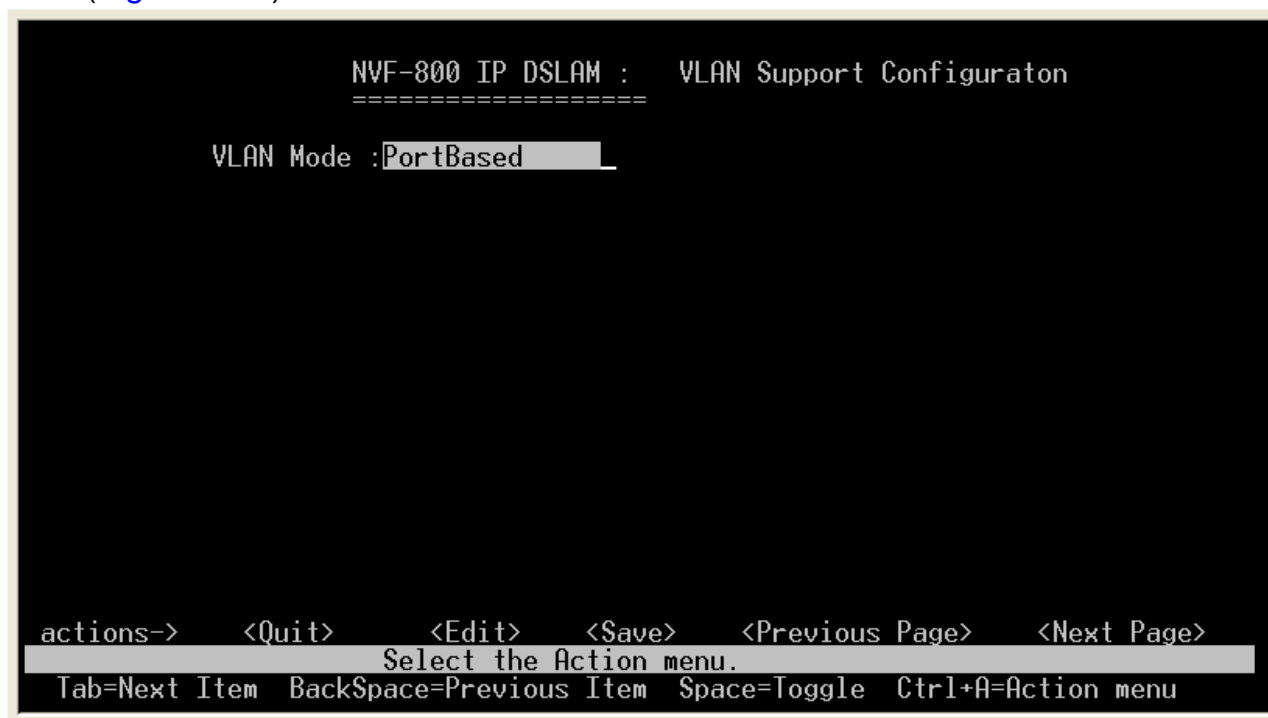


Figure 4.23 VLAN Mode: Port Based

4.1.1.2.4.2 Create a VLAN Group

You can create a new VLAN Group. (Figure 4.24)

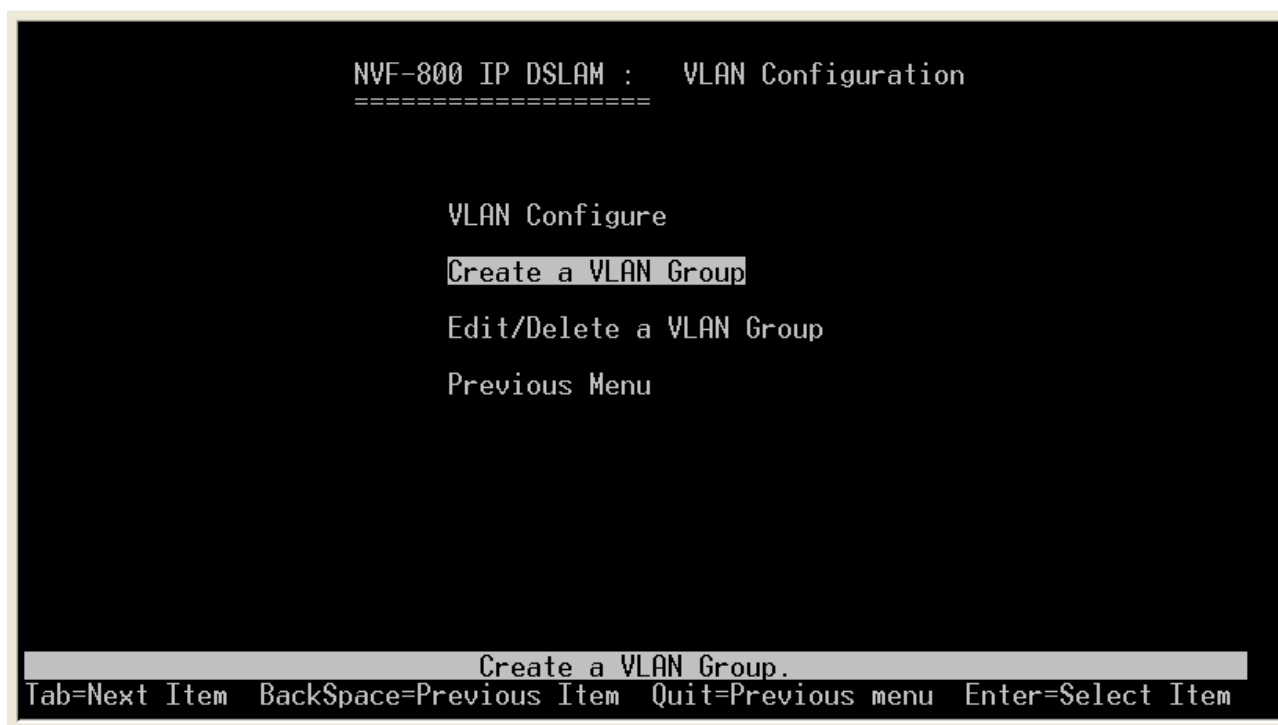


Figure 4.24 Create a VLAN Group

4.1.1.2.4.3 Edit/Delete a VLAN Group

Edit/Delete a VLAN Group. (Figure 4.25)

```
NVF-800 IP DSLAM :  VLAN Configuration
=====

VLAN Configure
Create a VLAN Group
Edit/Delete a VLAN Group
Previous Menu

Edit/Delete a VLAN Group.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
```

Figure 4.25 Edit or Delete a VLAN Group

4.1.1.2.5 Priority Configuration

Display or change port priority configuration. (Figure 4.26)

Item	Description
Priority 0 to 7:	Shows the priority if it is either low or high.
High/Low Queue Service Ratio H/L:	Shows the ratio of the priority high/low.

```

NVF-800 IP DSLAM : Priority Configuration
=====

Priority 0 : Low
Priority 1 : Low
Priority 2 : Low
Priority 3 : Low
Priority 4 : High
Priority 5 : High
Priority 6 : High
Priority 7 : High

High/Low Queue Service Ratio H:L :[5:1 ]

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 4.26 802.1p QoS(Quality of Service) Priority Configuration

4.1.1.2.6 MAC Address Configuration

Select the "Mac Address Configuration". The menu below includes the sub-menus of **Static Mac Address** and **Filtering Mac Address** (Figure 4.27)



Figure 4.27 Static Mac Address Configuration

4.1.1.2.6.1 Static MAC Address

Configure the Static MAC address. (Figure 4.28)

```

NVF-800 IP DSLAM :  Static MAC Address Configuration
=====
Mac Address      Port num          Mac Address      Port num
-----

```

actions-> <Add> <Edit> <Delete> <Save> <Quit>

Add/Edit/Delete static MAC addresses.

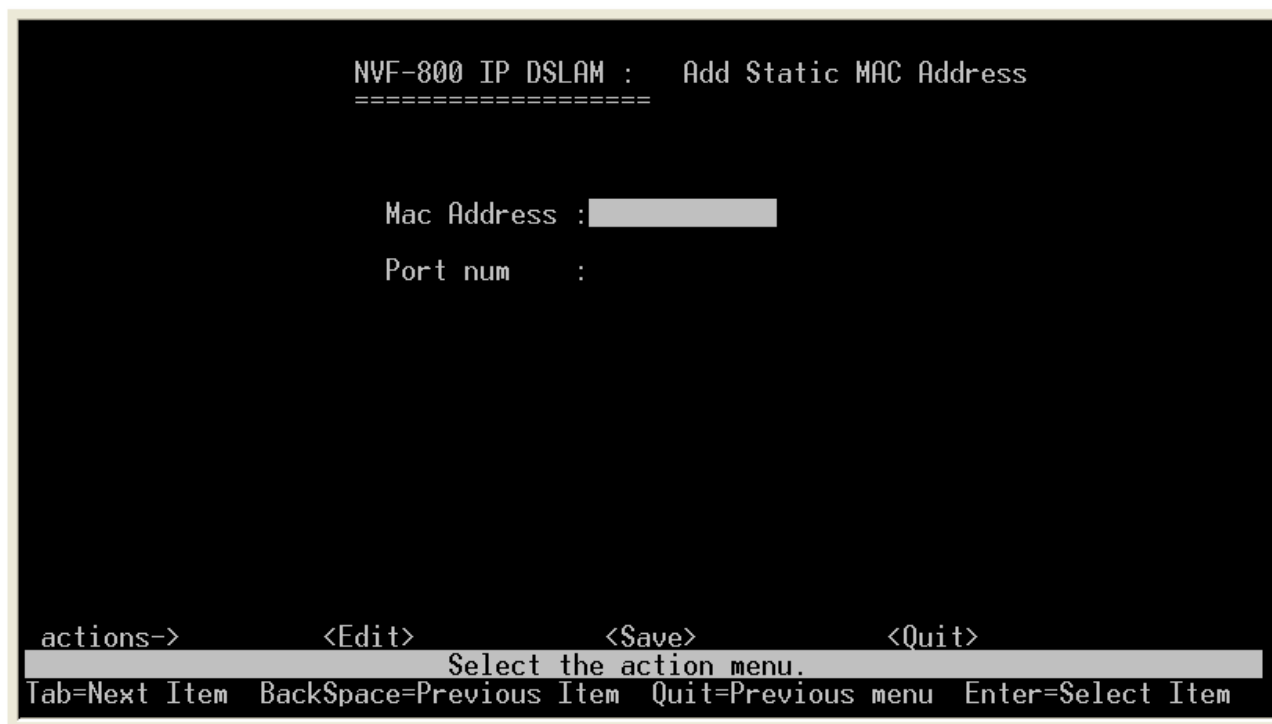
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item_

Figure 4.28 Static Mac Address Configuration

4.1.1.2.6.1.1 Add Static MAC Address

Add Static MAC Address(Figure 4.29)

Item	Description
Mac Address:	Input static MAC address for the selected port number.
Port num:	Input port number for the set static MAC address. Valid Range is from 1 to 10.



```

NVF-800 IP DSLAM :  Add Static MAC Address
=====

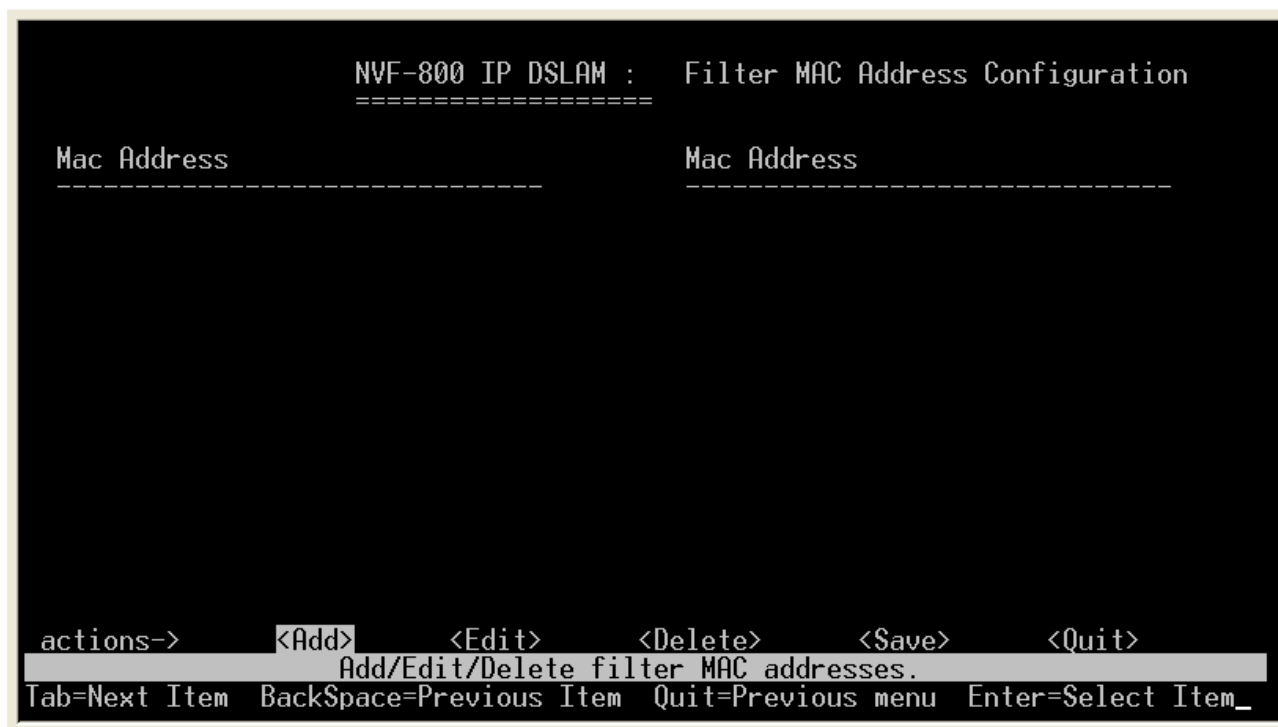
Mac Address : 
Port num   :

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
  
```

Figure 4.29 Add Static Mac Address

4.1.1.2.6.2 Filtering MAC Address

Filtering the MAC address configuration. (Figure 4.30)



```

NVF-800 IP DSLAM :  Filter MAC Address Configuration
=====

Mac Address          Mac Address
-----

actions->  <Add>    <Edit>    <Delete>    <Save>    <Quit>
Add/Edit/Delete filter MAC addresses.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item_
  
```

Figure 4.30 Filter Mac Address

Tip:

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if your network is congested because of high utilization from one MAC address, you can filter all traffic transmitted from that MAC address, restoring network flow while you troubleshoot the problem.

4.1.1.2.6.2.1 Add Filtering MAC Address

Item	Description
Mac Address:	Input the MAC address of certain device to be filtered out.

(Figure 4.31)



The screenshot shows a terminal-style interface with a black background and white text. At the top, it says "NVF-800 IP DSLAM : Add Filter MAC Address" followed by a line of equals signs. Below this, there is a prompt "Mac Address :" followed by a white rectangular input field. At the bottom, there is a menu bar with the text "actions->" followed by four options: "<Edit>", "<Save>", and "<Quit>". Below the menu bar, there is a line of text that says "Select the action menu." and another line of text that says "Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item".

Figure 4.31 Add Filter Mac Address

4.1.1.2.7 Misc Configuration

Select the "Misc Configuration". The menu below includes the sub-menus of **Port Security**, **Mac Age interval**, **Broadcast Storm Filtering** and **Max bridge transmit delay bound**. Please configure the miscellaneous items as follows. (Figure 4.32)

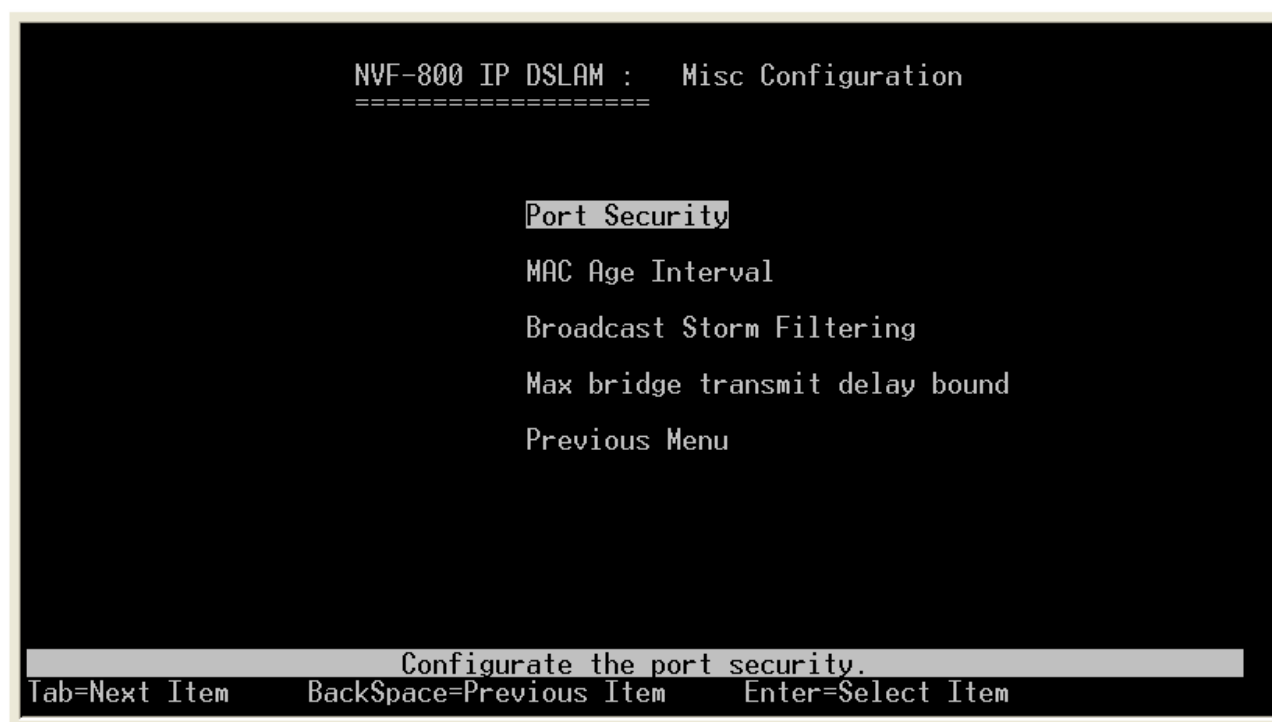


Figure 4.32 Select "Misc Confiruration"

4.1.1.2.7.1 Port Security

Configure the port security. (Figure 4.33)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
Enable Security:	Enable or disable for Port security.

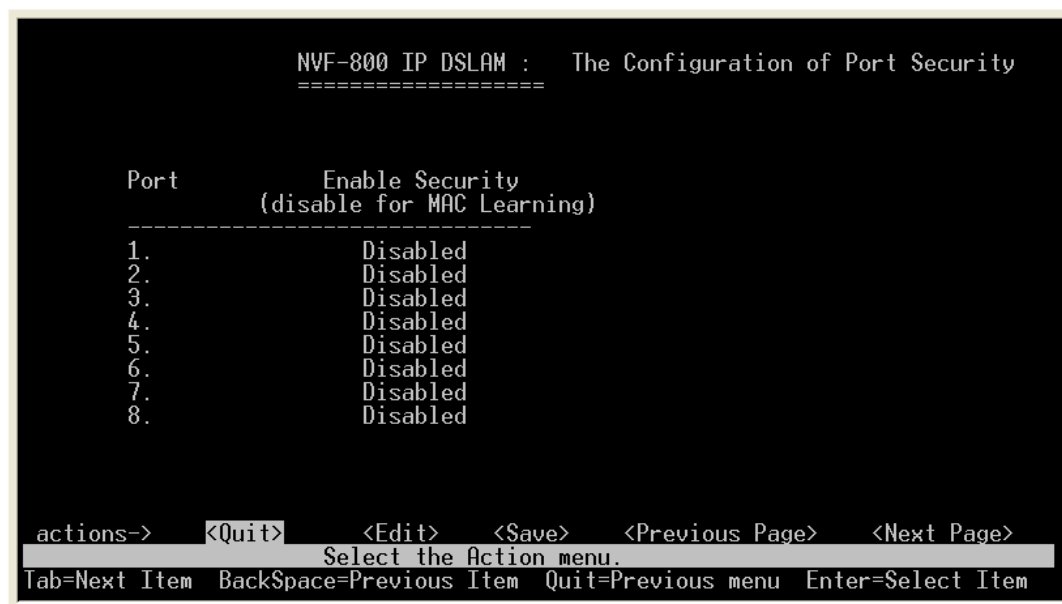


Figure 4.33 Port Security

Tip:

A port in security mode will be “locked” without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. enter the settings, then choice save the changes on this page.

4.1.1.2.7.2 MAC Age Interval

Configure the MAC aging time. (Figure 4.34)

Item	Description
MAC Age Interval:	MAC aging interval is from 300 to 765 seconds.



Figure 4.34 Mac Aging Time Configuration

Note:

If not set the aging-time, ip address and mac address mapping will be always there, even for a computer using the same ip to access does not automatically update the mac table. After setting the aging-time, every time of Aging time interval will arrive to relearn the MAC address table.

In fact, this time does not need special setting, default MAC age interval is **300** seconds.

4.1.1.2.7.3 Broadcast Storm Filtering

To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. (Figure 4.35)

Item	Description
Broadcast Storm Filter Mode:	Broadcast storm filter mode can either be 5%, 10%, 15%, 20%, 25% or NO. Default broadcast storm filter is at 5%.



Figure 4.35 Broadcast Storm Filter mode

4.1.1.2.7.4 Max Bridge Transmit Delay Bound

Configure the maximum bridge transmit delay bound. Default maximum bridge transmit delay bound is 4 seconds. (Figure 4.36)

Item	Description
Max bridge transmit delay bound:	Limit the packets queuing time in switch. If enable, the packets queued exceed will be drop. This valid value are 1sec, 2 sec,3sec, 4 sec and off.
Enable Delay Bound:	Delay bound can either be Enable or Disable.
Maximum Delay Time:	Maximum delay time is from 1ms to 255ms. Disabled is 0.

```

und          NVF-800 IP DSLAM :  Configure Max Bridge Transmit Delay Bo
=====

Max bridge transmit delay bound :4 Sec
Enable Delay Bound :Disabled
Max Delay Time :0

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

```

Figure 4.36 Configure the maximum bridge transmit delay bound.

4.1.1.3 Protocol Related Configuration

Select the "Protocol Related Configuration". The menu below includes the sub-menus of **STP**, **SNMP**, **GVRP** and **LACP**. (Figure 4.37)

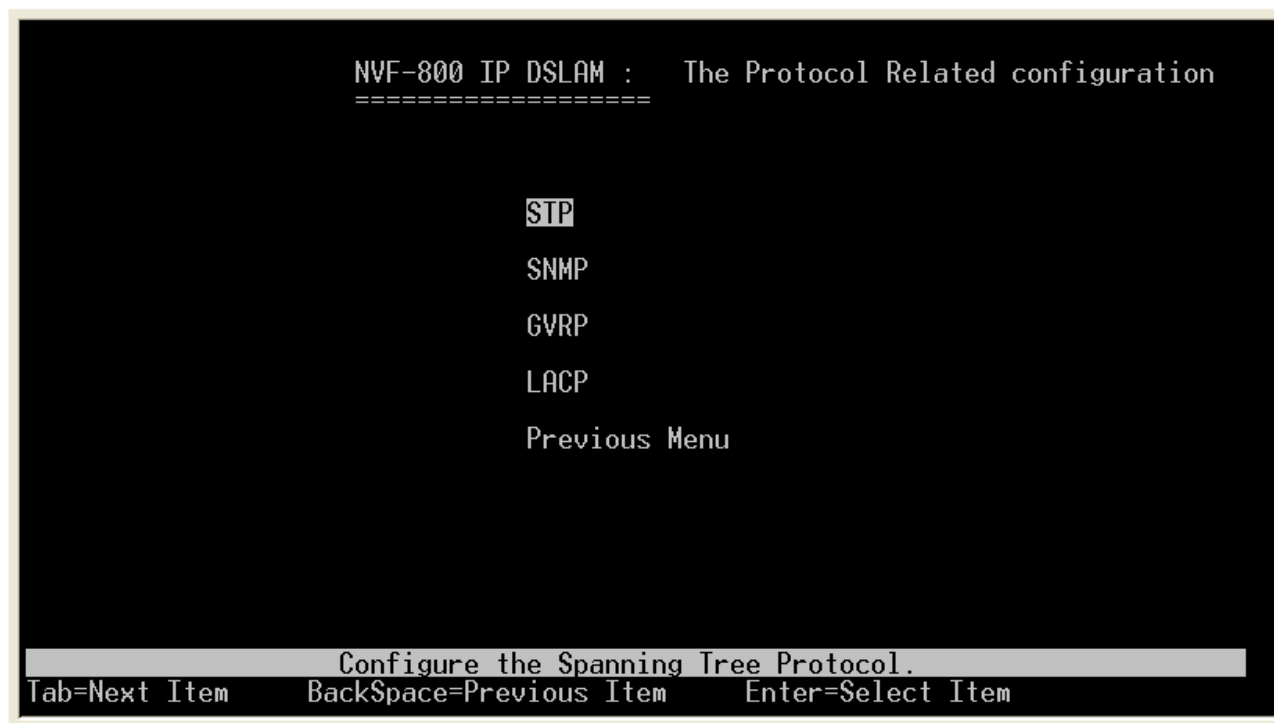


Figure 4.37 Configure the Protocol Related

4.1.1.3.1 STP

Select the "STP". The menu below includes the sub-menus of **STP Enable**, **System Configuration** and **Perport Configuration**.

(Figure 4.38)

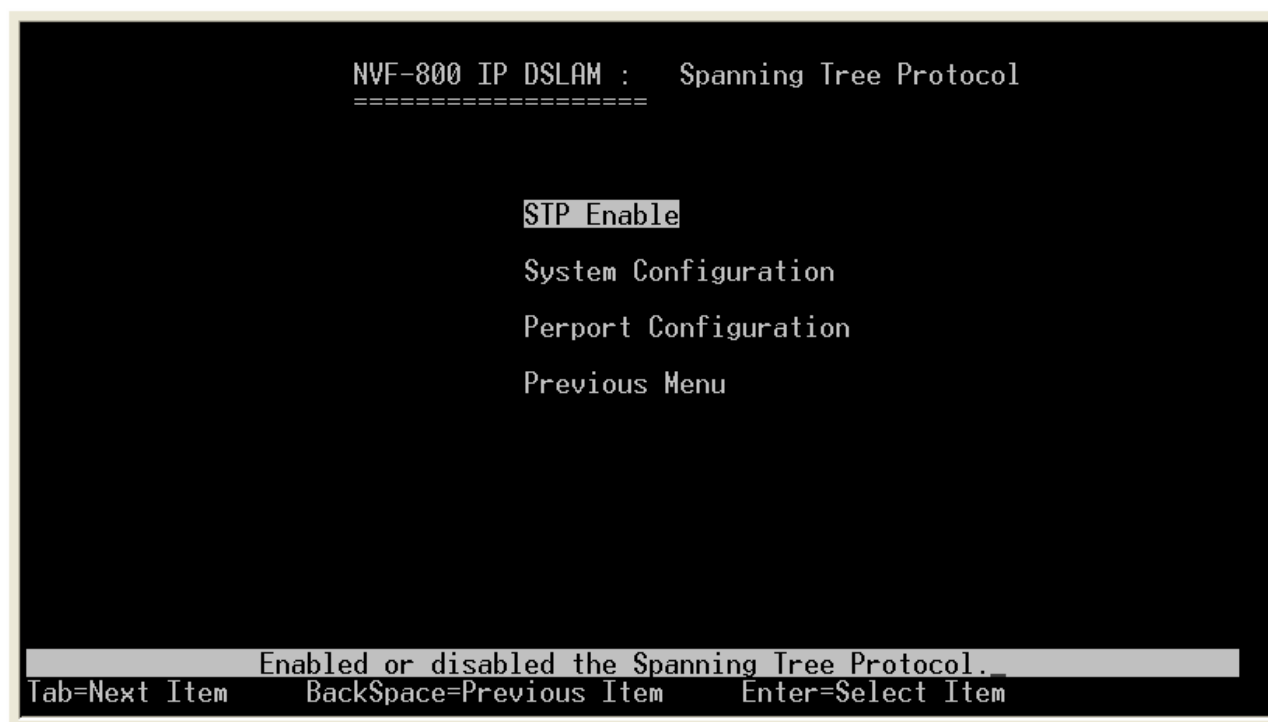


Figure 4.38 Spanning Tree configuration

4.1.1.3.1.1 STP Enable

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1d) for used to prevent forwarding loops on a LAN. When STP enabled, to ensure that only one path at a time is active between any two nodes on the network. (Figure 4.39)

We are recommended that you enable STP on all switches ensures a single active path on the network.

Item	Description
STP:	Spanning Tree Protocol can either be enabled or disabled.

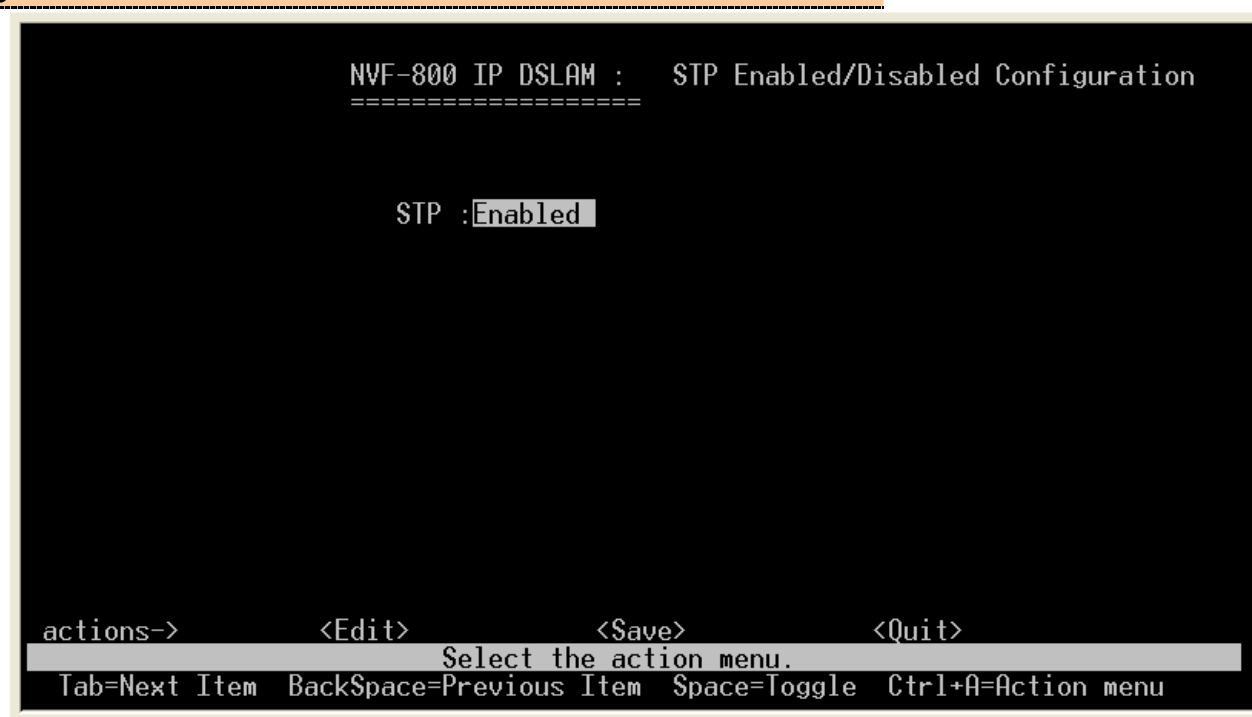


Figure 4.39 STP Enable / Disable

4.1.1.3.1.2 System Configuration

Configure the STP system information. (Figure 4.40)

Item	Description
Priority:	A priority value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Valid input priority range is from 1 to 65535. Default priority is 32768 .
Max Age:	The number of seconds a bridge waits without receiving . Spanning-Tree Protocol configuration messages before attempting a reconfiguration.Valid input max age range is from 6 to 40. Default max age is 20 .
Hello Time:	The number of seconds between the transmission of Spanning-Tree Protocol configuration messages.Valid input hello time range is from 1 to 10. Default hello time is 2
Forward Delay Time:	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.Valid input forward delay time range is from 4 to 30. Default forward delay time is 5 .

```

NVF-800 IP DSLAM : STP System Configuration
=====

Root Bridge Information          Configure Spanning Tree Parameters
-----
Priority      : 32768            Priority (1-65535)   :32768
Mac Address   : 004063800030    Max Age (6-40)      :15
Root_Path_Cost : 0              Hello Time (1-10)   :2
Root Port     : Root           Forward_Delay_Time(4-30) :5
Max Age       : 15
Hello Time    : 2
Forward Delay : 5

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 4.40 STP System Configuration

4.1.1.3.1.3 Perport Configuration

Configure the STP per port configuration. Default pathcost is 10 and priority is 128. (Figure 4.41)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
PortState:	Shows the condition of the port if it is enabled or disabled.
PathCost:	Specifies the path cost of the port that switch uses to determine which port are the forwarding ports the lowest number is forwarding ports, the rage is 1-65535 and default value base on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10
Priority:	You can make it more or less likely to become the root port, the range is from 0 to 255,default setting is 128, the lowest number has the highest priority.

NVF-800 IP DSLAM : STP Port Configuration			
Port	PortState	PathCost	Priority
1.	Disabled	10	128
2.	Disabled	10	128
3.	Disabled	10	128
4.	Disabled	10	128
5.	Disabled	10	128
6.	Disabled	10	128
7.	Disabled	10	128
8.	Disabled	10	128
actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>			
Select the Action menu.			
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item			

Figure 4.41 STP Port Configuration

4.1.1.3.2 SNMP

Select the "SNMP". The menu below includes the sub-menus of **System Options**, **Community Strings** and **Trap Mangers**. SNMP means Simple Network Manager Protocol. (Figure 4.42)

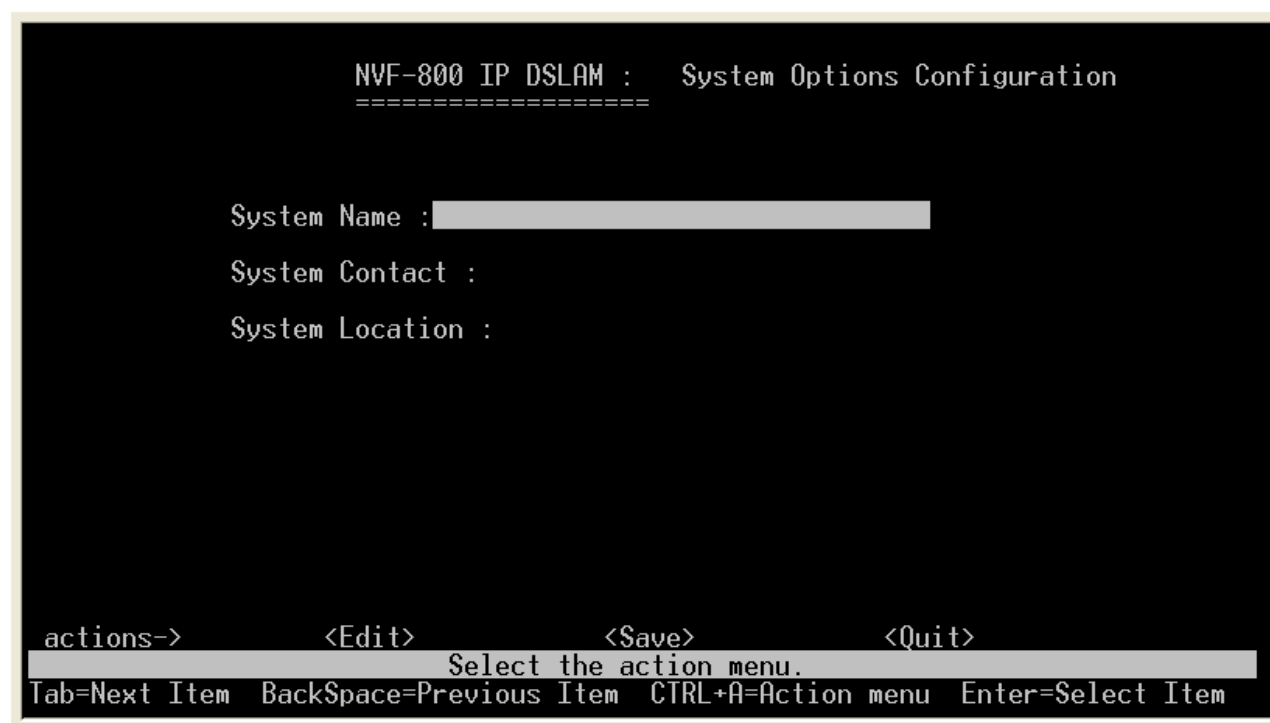


Figure 4.42 SNMP Configuration

4.1.1.3.2.1 System Options

Configure the system information. (Figure 4.43)

Item	Description
System Name:	Configuration to your own system name up to 32 characters.
System Contact:	Configuration to your own system contact up to 32 characters. (i.e. a person or organization)
System Location:	Configuration to your own system location up to 32 characters.



```

NVF-800 IP DSLAM :  System Options Configuration
=====

System Name : 
System Contact : 
System Location : 

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  CTRL+A=Action menu  Enter=Select Item
  
```

Figure 4.43 System Options Configuration

4.1.1.3.2.2 Community Strings

Configure the community. (Figure 4.44)

For example, community name set to “public”, Write access set to “Restricted”, means enable requests accompanied by this string to display MIB-object information. And another community name set to “private”, Write access set to “Unrestricted”, means enable requests accompanied by this string to display MIB-object information and to set MIB objects.

```

NVF-800 IP DSLAM :  SNMP Community Configuration
=====
Community Name      Write Access
-----
public              Restricted

actions->  <Add>    <Edit>    <Delete>    <Save>    <Quit>
Add/Edit/Delete community strings.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item_

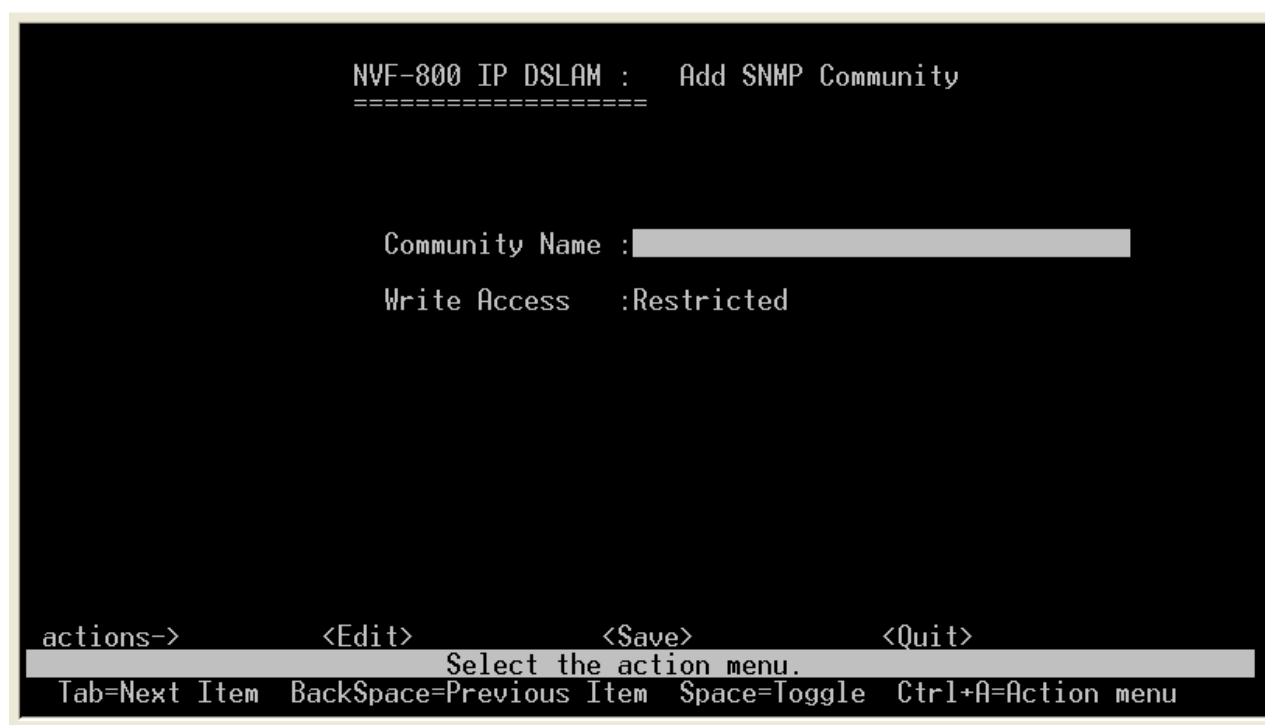
```

Figure 4.44 SNMP Community Configuration

4.1.1.3.2.2.1 Add SNMP Community

Add SNMP community. (Figure 4.45)

Item	Description
Community Name:	Input valid community name up to 32 characters to be included in the SNMP community.
Write Access:	Write access can either be restricted or unrestricted.



```

NVF-800 IP DSLAM :  Add SNMP Community
=====

Community Name : 
Write Access   :Restricted

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

```

Figure 4.45 Add SNMP Community

4.1.1.3.2.3 Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the IP DSLAM. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string. (Figure 4.46)

```

NVF-800 IP DSLAM :  Trap Managers Configuration
=====
IP                      Community Name
-----
192.168.16.10          public

actions->      <Add>      <Edit>      <Delete>      <Save>      <Quit>
Add/Edit/Delete trap managers.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item_

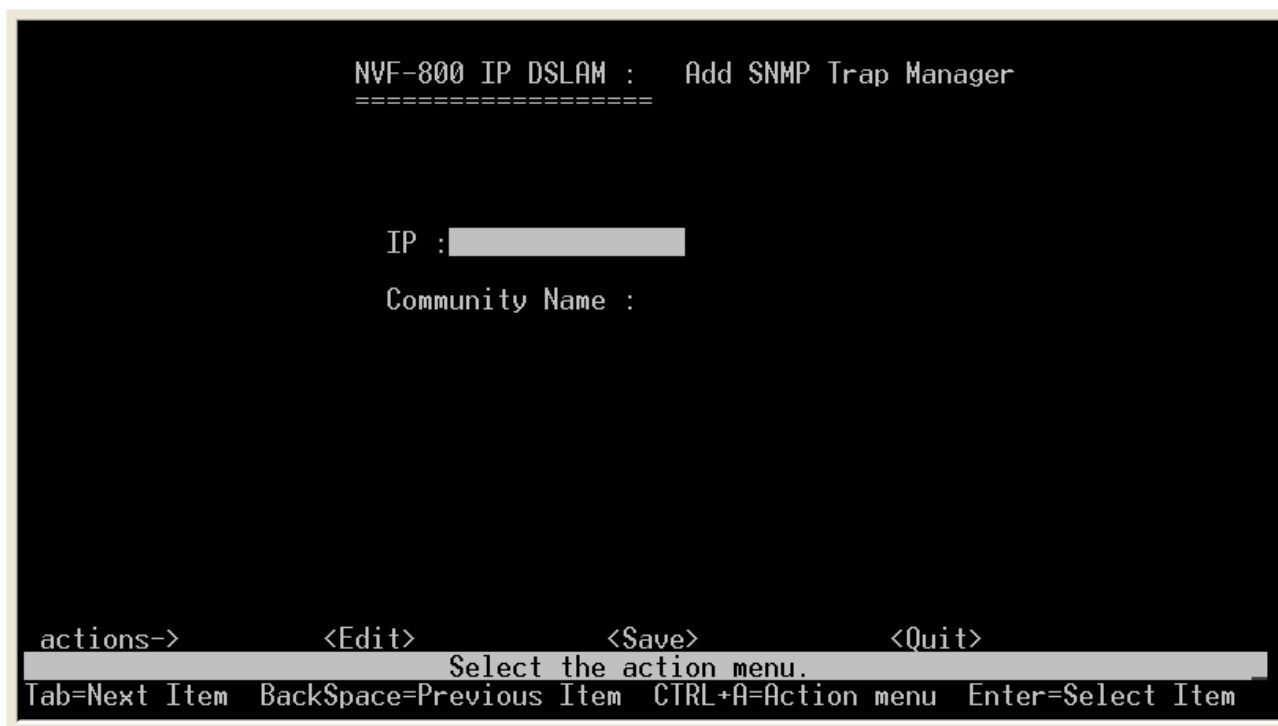
```

Figure 4.46 Trap Managers Confiruration

4.1.1.3.2.3.1 Add SNMP Trap Manager

Add SNMP trap manager. (Figure 4.47)

Item	Description
IP:	Input IP address to be included in the SNMP trap manager.
Community Name:	Input valid community name up to 32 characters to be included in the SNMP trap manager.



```

NVF-800 IP DSLAM :  Add SNMP Trap Manager
=====

IP : 
Community Name :

actions->      <Edit>      <Save>      <Quit>
Select the action menu.

Tab=Next Item  BackSpace=Previous Item  CTRL+A=Action menu  Enter=Select Item

```

Figure 4.47 Add SNMP Trap Manager

4.1.1.3.3 GVRP

Default GVRP is disabled. (Figure 4.48) Please refer to section 4.1.1.2.4.1 VLAN Configure.

Item	Description
GVRP:	GARP VLAN Registration Protocol can either be enabled or disabled.

```

NVF-800 IP DSLAM :  GVRP Configuration
=====

GVRP : Disabled

actions->          <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next ItememBackSpace=Previous ItememQuit=Previous menuEnter=Select Item

```

Figure 4.48 GVRP Configuration Enable / Disable

4.1.1.3.4 LACP

Select the "LACP ". The menu below includes the sub-menus of **Aggregator Setting**, **State Activity** and **LACP Status**.

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE802.3ad. ([Figure 4.49](#))

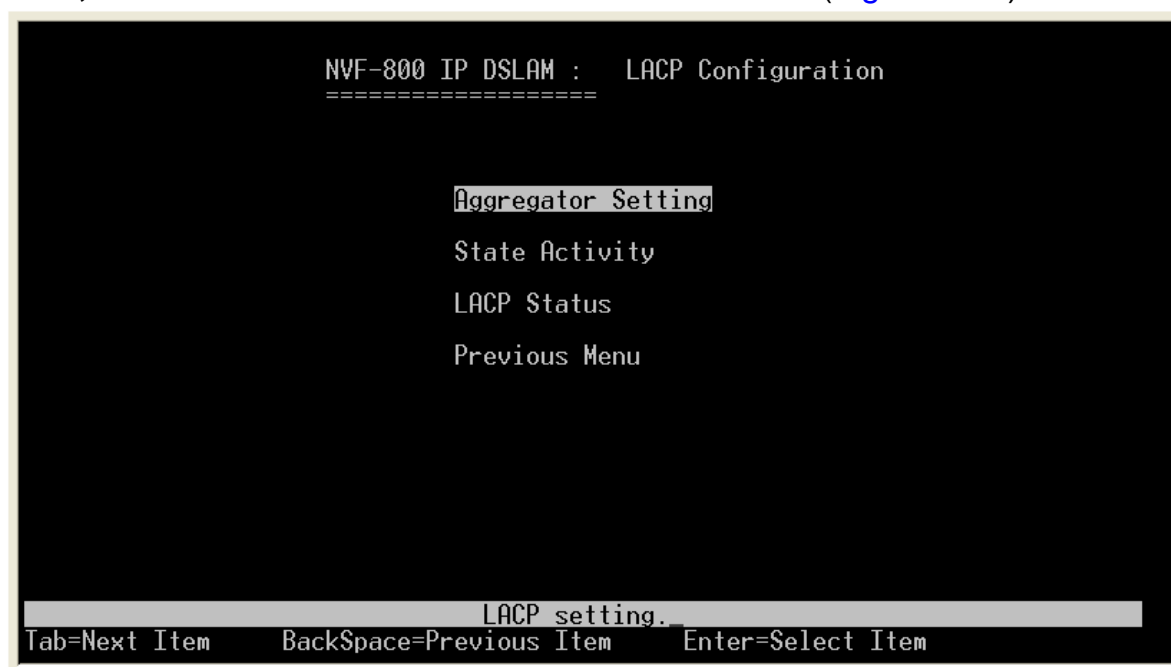


Figure 4.49 LACP Configuration

4.1.1.3.4.1 Aggregator Setting

LACP setting. (Figure 4.50)

```

NVF-800 IP DSLAM :  LACP Group Configuration
=====

Group      LACP      LACP Work Port Num
-----

actions->  <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next ItememBackSpace=Previous ItememQuit=Previous menuEnter=Select Item

```

Figure 4.50 LACP Group Configuration

4.1.1.3.4.2 State Activity

Configure the state activity. (Figure 4.51)

Item	Description
Port:	Shows the port number of NVF-800S VDSL IP DSLAM.
State Activity:	State Activity for LACP can either be active or passive.

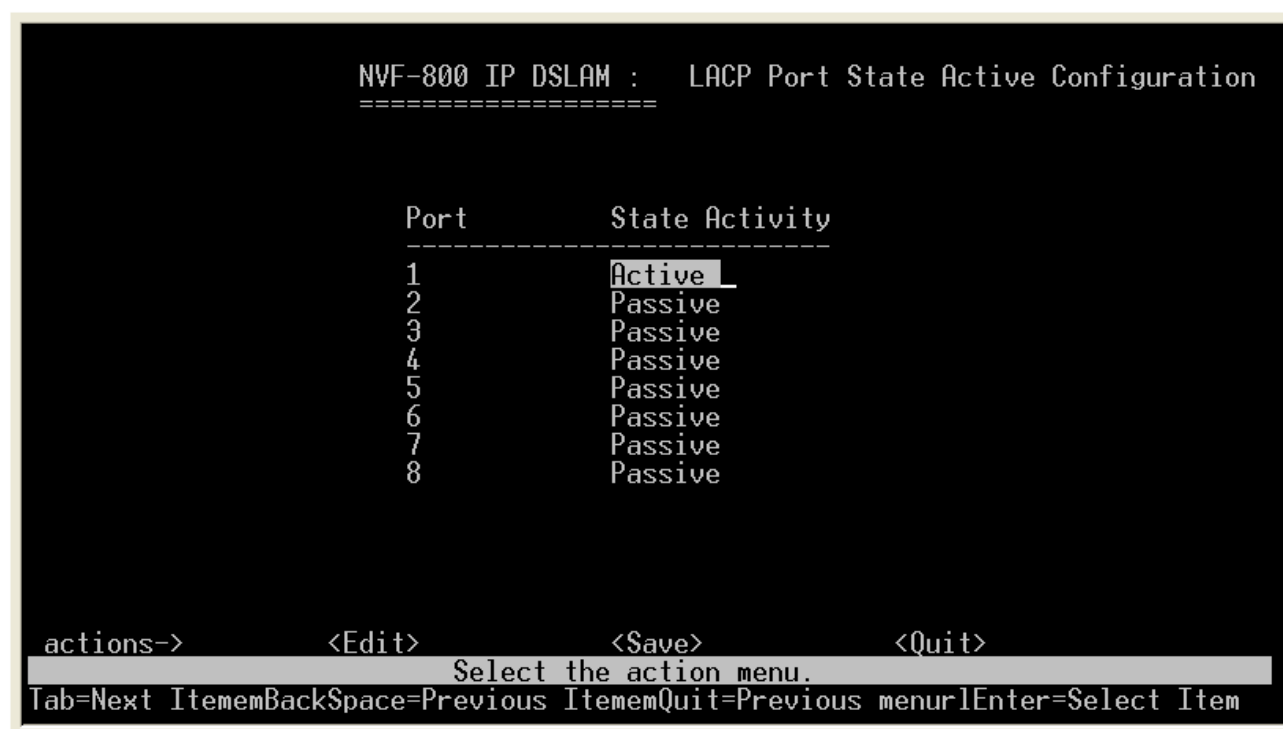


Figure 4.51 LACP Port State Active Configuration

4.1.1.3.4.3 LACP Status

Show the LACP status. This page is no group active. LACP don't working. ([Figure 4.52](#))

```

NVF-800 IP DSLAM :   LACP Group Status
=====

NO GROUP ACTIVE

actions->      <Quit>      <Previous Page>      <Next Page>
               Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item_
  
```

Figure 4.52 LACP Group Status

4.1.1.4 Temperature and Fan Monitor

Display the temperature in degrees Celsius(℃) and fan monitor in RPM. (Figure 4.53)

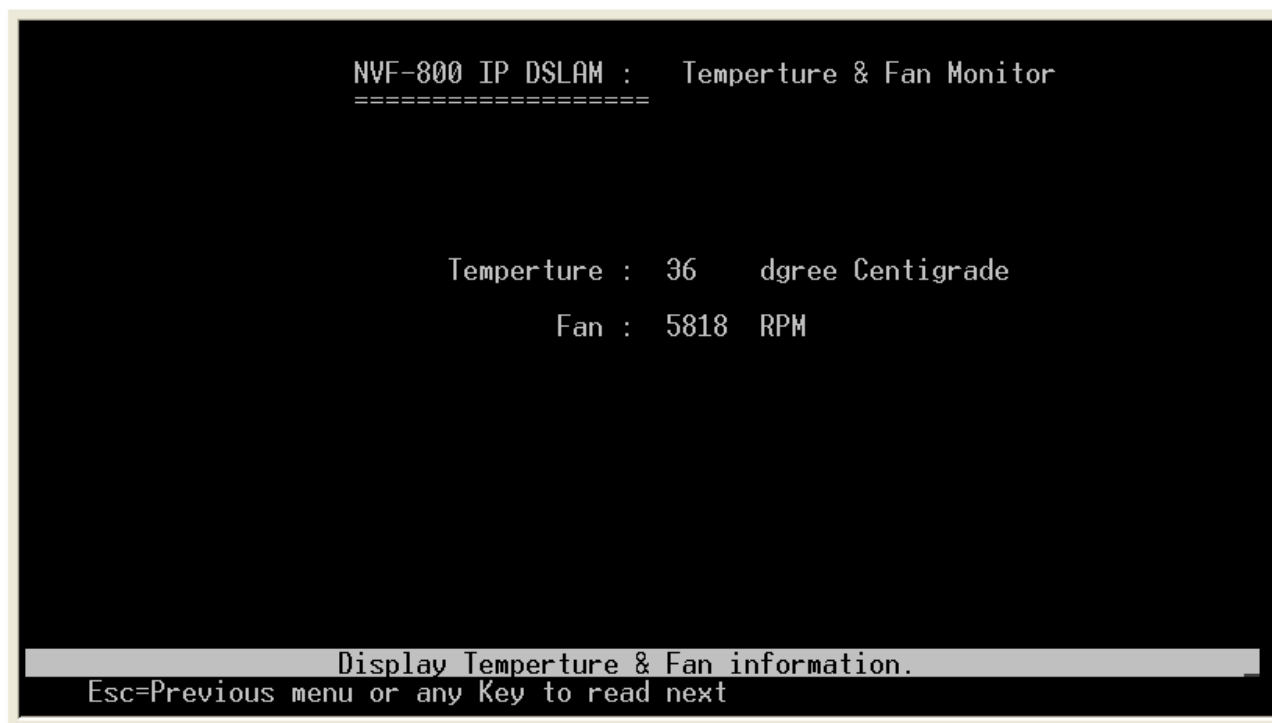


Figure 4.53 Temperature & FAN Monitor

4.1.1.5 Reboot Switch

Select the "Restart ". The menu below includes the sub-menus of **Default** and **Restart**.(Figure 4.54)



Figure 4.54 Restart Configuration

4.1.1.5.1 Default

Recovering to default. ([Figure 4.55](#))

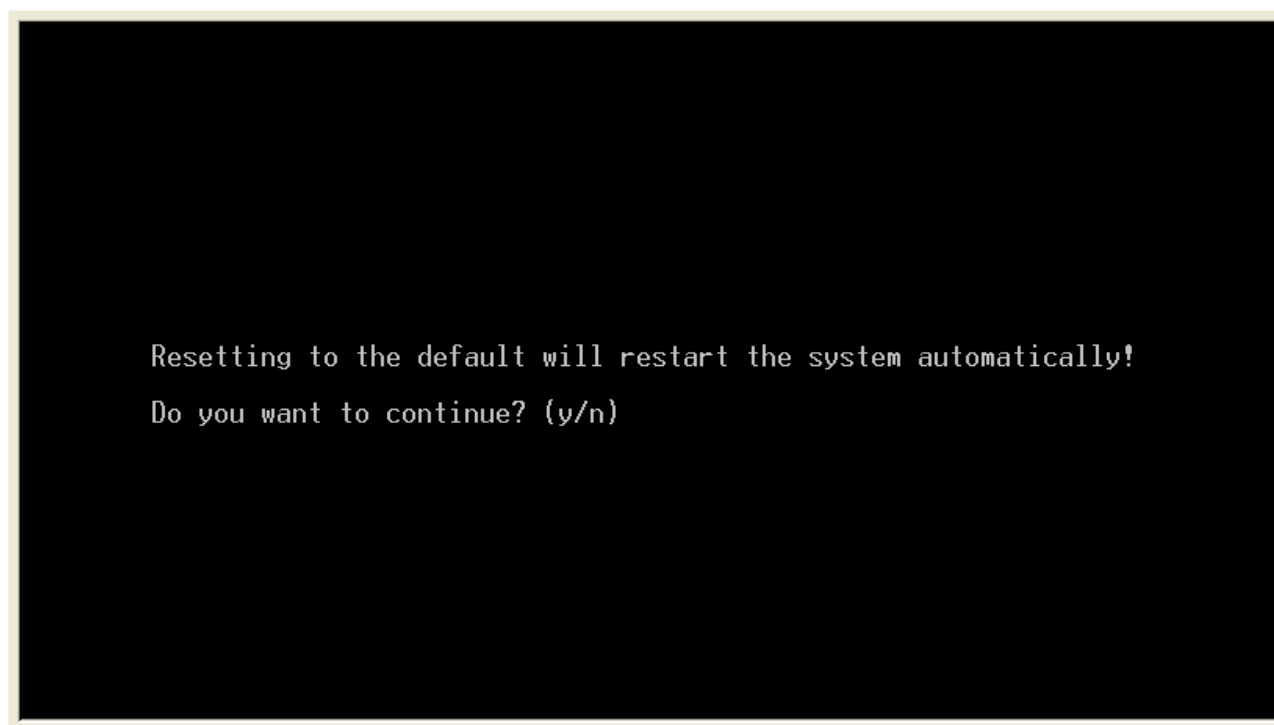


Figure 4.55 Resetting to the default system

Caution:

1. All settings will return to factory defaults.
2. After set to default system, please reboot the system.

Choose “**Yes**”

Reset the system to default automatically. ([Figure 4.56](#))

If No, It will go back to the previous menu.

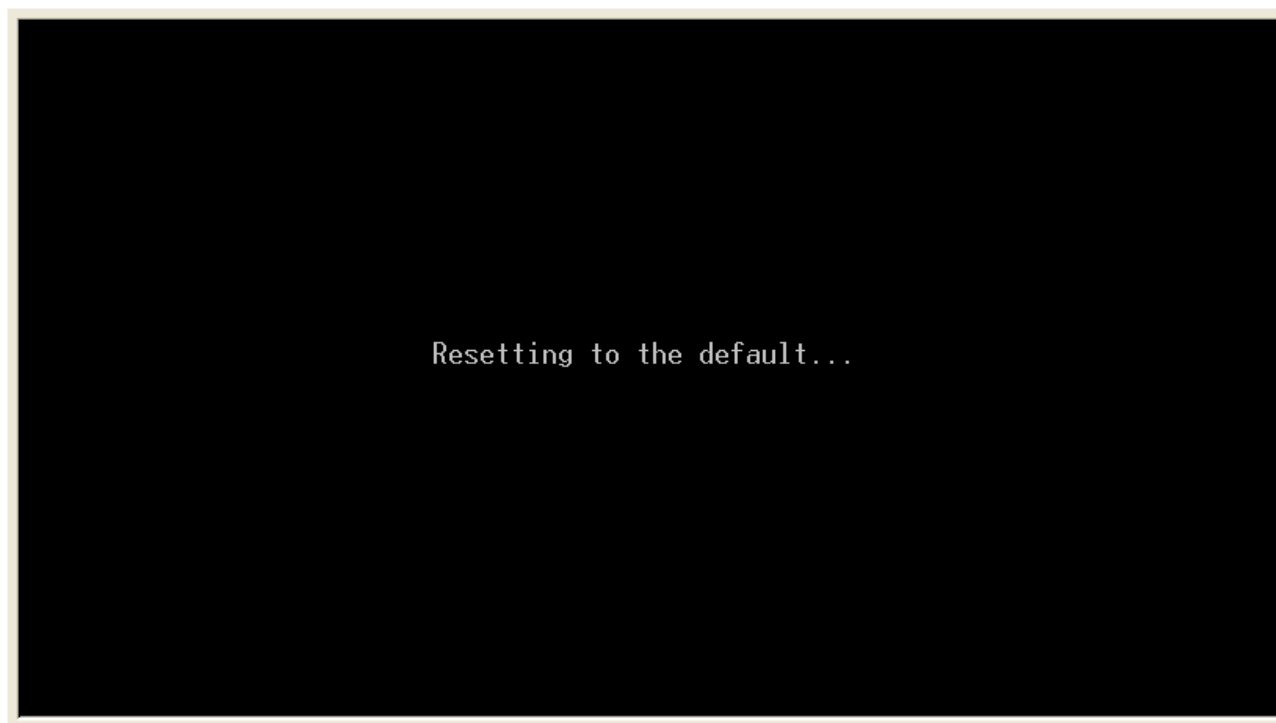


Figure 4.56 Resetting to the default

4.1.1.5.2 Reboot Switch

Restart the system. (Figure 4.57)

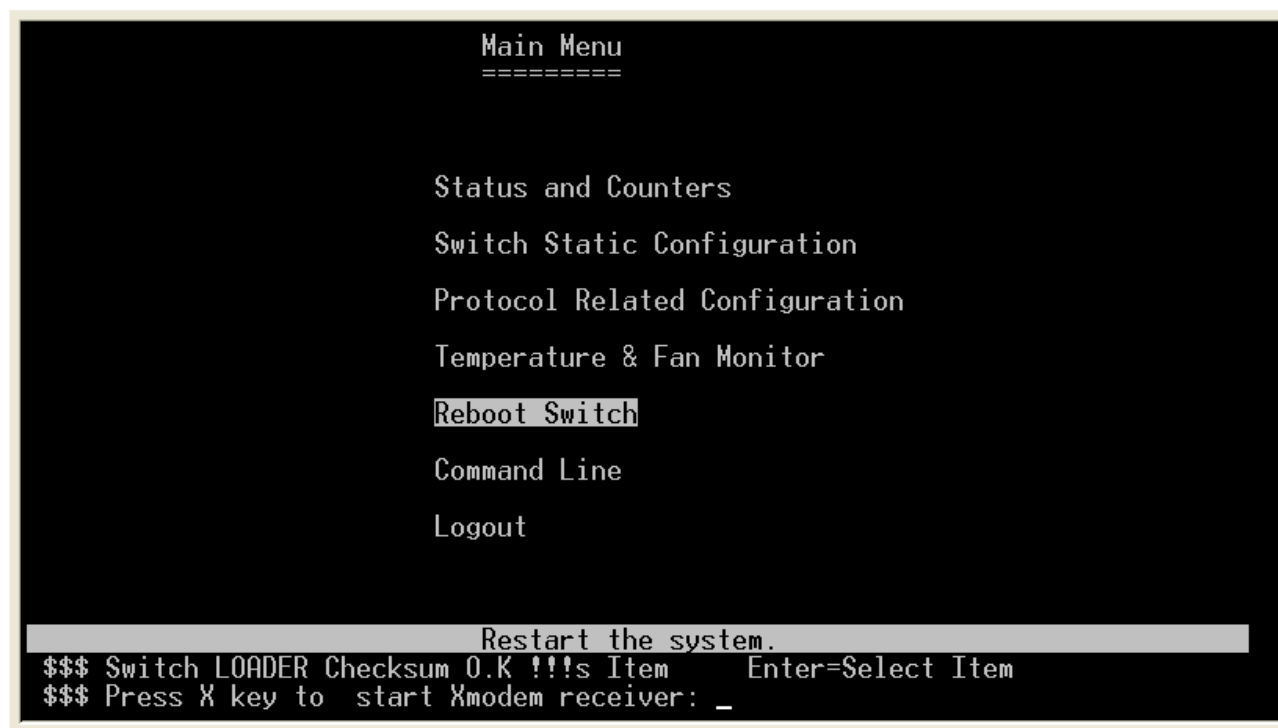


Figure 4.57 Reboot Switch

4.1.1.6 Command Line

Command Line. (Figure 4.58)



Figure 4.58 Command Line

Caution:

1. This function is only used to debug for the engineer.
2. If you want to exit the command line, please input "**quit**", then press "enter" key to exit the command line.

4.1.1.7 Logout

Exit this user interface program.([Figure 4.59](#))



Figure 4.59 Logout

4.2 Remote Network Management

4.2.1 IP Setting

Setup the “IP Address” with the local serial console port (RS-232 Port) then use this IP address to control the VDSL IP DSLAM by **Telnet** and **WEB**. Then use the default IP address to control this VDSL IP DSLAM.

1. Remote control by “Telnet”

To enter Telnet, type the IP address of the NVF-800S to connect management system then type User name and Password.

Default User Name: admin

Default Password: 123

Note:

1. For security reason, we limit the user login number on Telnet and Console port. So you can't login Telnet and Console port at the same time. But you can login Telnet and Console port at the different time.
2. WEB Login doesn't limit user login numbers.
When you want to close console port control you must log-out to leave. Otherwise you can't login by Telnet.

2. Network control by “WEB”

4.2.2 Web Management Function

1. Provide a Web browser to manage and monitor the NVF-800S, the default values as follows:
If you need change IP address in first time, use console mode to modify it.

IP Address: 192.168.16.250

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.16.1

User Name: admin

Password: 123

2. Browse “[http:// 192.168.16.250](http://192.168.16.250)”, type user name and password as above. (Figure 4.60)

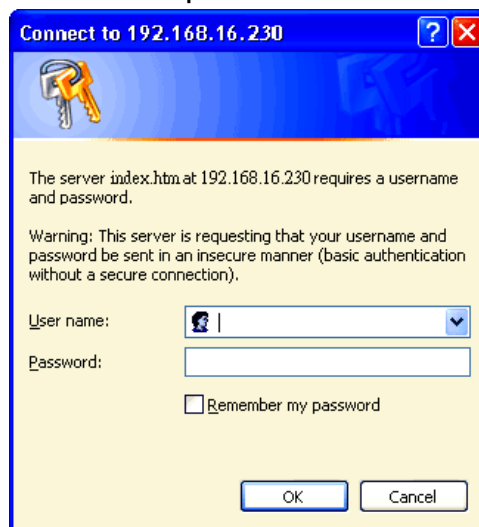


Figure 4.60 Username & Password

4.2.2.1 Web Management Home Overview

This is VDSL Home Page. (Figure 4.61)

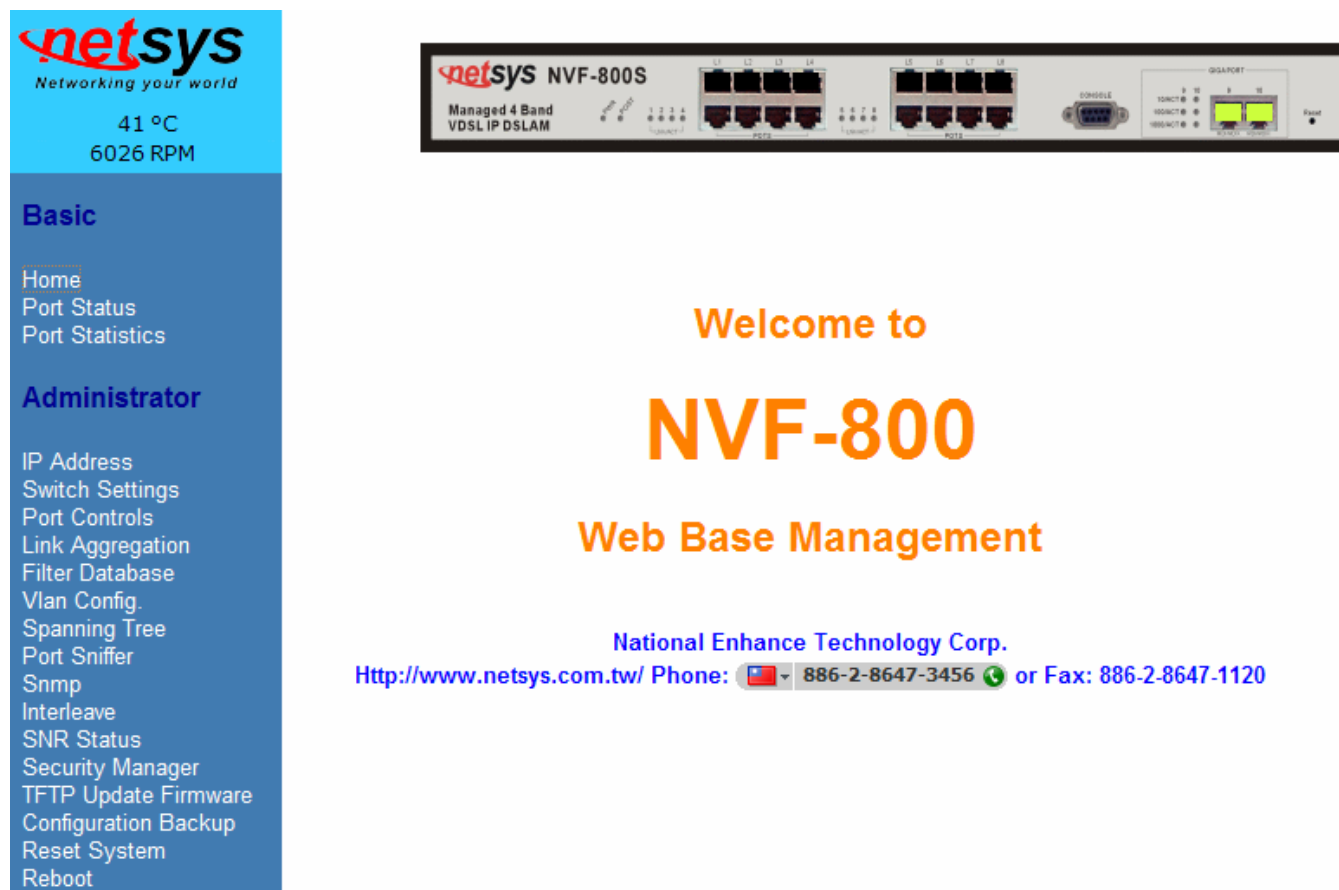


Figure 4.61 Web Base Management

4.2.2.2 Port Status

1. This page can see the status of every port. (Figure 4.62)

Item	Description
State: Display port status enable or disable state, where enable is link port and disable is no link port. Config: Display the user setup setting On when enable and Off when disable. Actual: Display the negotiation result.	
Link Status: Down is "No Link", Up is "Link"	
Auto Negotiation: NVF-800S auto negotiation mode Configure: Display the user setup of auto negotiation mode. Actual: Display the negotiation result.	
Speed status: Port 9 、 10 are 10/100/1000Mbps or and Port 1- 8 are 5/15/25Mbps. Configure: Display the state of user setup. Actual: Display the negotiation result.	
Duplex status: Display full-duplex or half-duplex mode. Configure: Display the user setup. Actual: Display the negotiation result.	
Flow control: Display flow control status enable or disable mode. Configure: Display the user setup. Actual: Display the negotiation result.	

Port Status

The following information provides a view of the current status of the unit.

Port Num	State		Link Status	Auto Negotiation		Speed Status		Duplex Status		Flow Control	
	Config	Atual		Config	Atual	Config	Atual	Config	Atual	Config	Atual
1	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
2	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
3	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
4	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
5	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
6	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
7	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
8	On	Off	Down	Auto	Auto	Auto	5M	Full	Full	On	On
9	On	On	Up	Auto	Auto	1000	100	Full	Full	On	On
10	On	On	Up	Auto	Auto	1000	100	Full	Full	On	On

Figure 4.62 Port Status

4.2.2.3 Port Statistics

1. The following information provides a view of the current status of the unit. (Figure 4.63)

Port Statistics

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1	Off	Down	0	0	0	0	0	0	0
2	Off	Down	0	0	0	0	0	0	0
3	Off	Down	0	0	0	0	0	0	0
4	Off	Down	0	0	0	0	0	0	0
5	Off	Down	0	0	0	0	0	0	0
6	Off	Down	0	0	0	0	0	0	0
7	Off	Down	0	0	0	0	0	0	0
8	Off	Down	0	0	0	0	0	0	0
9	On	Up	3168	0	2830	0	0	0	26
10	On	Up	0	0	764	0	0	0	103

Figure 4.63 Port Statistics

4.2.2.4 Administrator

There are many management functions include:

IP Address: Set IP Addresses. See section 4.2.2.4.1

Switch Setting: See section 4.2.2.4.2

Console Port Information: See section 4.2.2.4.3

Port Controls: See section 4.2.2.4.4

Link Aggregation: See section 4.2.2.4.5

Filter Database: See section 4.2.2.4.6

VLAN Config.: See section 4.2.2.4.7

Spanning Tree: See section 4.2.2.4.8

Port Sniffer: See section 4.2.2.4.9

SNMP: See section 4.2.2.4.10

Interleave: See section 4.2.2.4.11

SNR Status: See section 4.2.2.4.12

Security Manager: See section 4.2.2.4.13

TFTP Update Firmware: See section 4.2.2.4.14

Configuration Backup: See section 4.2.2.4.15

Restart System: See section 4.2.2.4.16

Reboot: See section 4.2.2.4.17

4.2.2.4.1 IP Address

1. User can configure the IP Settings and fill in the new value, then click the apply button.
2. User must reset NVF-800S and use new IP address to browse this web management. ([Figure 4.64](#))

Set IP Addresses

IP Address	192.168.16.243
Subnet_Mask	255.255.255.0
Gateway	192.168.16.1

Figure 4.64 Default IP is 192.168.16.250

4.2.2.4.2 NVF-800S Settings

4.2.2.4.2.1 Basic

(Figure 4.65)

Item	Description
Description:	Display the device type.
MAC Address:	The unique hardware address assigned by manufacturer.
Firmware Version:	Display the NVF-800S firmware version.
Hardware Version:	Display the NVF-800S hardware version.
Default config value version:	Display write to default EEPROM value tale version.

Switch Settings

Basic	Advanced
Description	NVF-800 8+2G Port IP DSLAM
MAC Address	004063800030
Firmware version	C.9
Hardware version	B.1
Default config value version	v26.00

Figure 4.65 Switch Settings Basic

4.2.2.4.2.2 Advanced

Miscellaneous Setting: (Figure 4.66)

Item	Description
MAC Address Age-out Time:	Type the number of seconds that an inactive MAC address will remain in the NVF-800S address table. The valid range is 300~765 seconds. Default is 300 seconds.
Max bridge transit delay bound control:	Limit the packets queuing time in NVF-800S. If enable, the packets will be drop if exceed the queued time. The valid values are 1sec, 2 sec, 4 sec and off. Default is 4 seconds.
Broadcast Storm Filter:	To configure broadcast storm filter, set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold being set, broadcast storm filter becomes active. The valid threshold values are 5%, 10%, 15%, 20%, 25% and off. The default value is 5%.

Switch Settings

Basic

Advanced

Enter the settings, then click Submit to apply the changes on this page.

☒ MAC Table Address Entry Age-Out Time: seconds

Max bridge transmit delay bound control:

Broadcast Storm Filter Mode:

Figure 4.66 Switch Settings Advanced (Miscellaneous Setting)

Priority Queue Service settings: (Figure 4.67)

Item	Description
First Come First Served:	The sequence of packets sent depends on arrived order.
All High before Low:	The high priority packets are sent before low priority packets.
Weighted Round Robin:	Select the preference given to packets in the NVF-800S high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example 5 High : 2 Low means that the NVF-800S sends 5 high priority packets before sending 2 low priority packet.
Enable Delay Bound:	Limit the low priority packets queuing time in NVF-800S. Default Max Delay Time is 255ms. If the low priority packet stays in NVF-800S exceed Max Delay Time, it will be sent. The valid range is 1~255 ms.
QoS Policy: High Priority Levels:	0~7 priority level can map to high or low queue.

Priority Queue Service:

☐ First Come First Served
☐ All High before Low
☒ WRR

High weight:
 Low weight:

☐ Enable Delay Bound
 Max Delay Time: ms

Qos Policy: High Priority Levels

☐ Level0
 ☐ Level1
 ☐ Level2
 ☐ Level3
 ☒ Level4
 ☒ Level5
 ☒ Level6
 ☒ Level7

Figure 4.67 Priority Queue Service

Protocol Enable Setting: (Figure 4.68)

Item	Description
Enable Spanning Tree Protocol:	Default recommends enable STP
Enable Internet Group Multicast Protocol:	Default recommends enable IGMP protocol
Enable Manage VDSL Switch from VDSL Ports:	Enable manage VDSL IPDSLAM from port 1~8
VLAN Operation Mode:	No VLAN 802.1Q(Tagging Based) without GVRP 802.1Q(Tagging Based) with GVRP Port Based VLAN
Auto Speed SNR Margin Maximun Value setup:	Auto Speed SNR Margin Maximun Value must be 35 ~ 50

Protocol Enable Setting

☒ Enable STP Protocol

☒ Enable IGMP Protocol

☐ Enable Manage VDSL Switch from VDSL Ports

VLAN Operation Mode: No VLAN

Auto Speed SNR margin value setup: Maximum 42 db

Figure 4.68 Protocol Enable Setting

Tip:

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)

GVRP allows automatic VLAN configuration between the NVF-800S and nodes. If the NVF-800S is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the NVF-800S, the NVF-800S will automatically add that device to the existing VLAN.

4.2.2.4.3 Console Port Information

Console is a standard UART interface to communicate with Serial Port.

User can use windows HyperTerminal program to link the NVF-800S. Connect To->Configure

Bits per seconds:	9600
Data bits:	8
Parity:	none
Stop bits:	1
Flow control:	none

4.2.2.4.4 VDSL Speed Control and port Enable/Disable

This section shows you how to change every port status and speed mode. ([Figure 4.69](#))

Item	Description
State:	You can disable or enable VDSL port control
Auto Negotiation:	You can set enable or disable VDSL port
Speed:	You can change VDSL Speed mode by 5Mbps, 15Mbps or 25Mbps. Speed Default Value: Auto-speed
Duplex:	User can set full-duplex or half-duplex mode for Ethernet port. VDSL port fixed on Full Duplex.
Flow Control:	Full: User can set flow control function enable or disable in full mode.
	Half: User can set backpressure enable or disable in half mode.

Auto Speed procedures:

- Confirm the phone cable been connected for both NVF-800S and NVF-200R.
- Powered on NVF-800S and NVF-200R.

- c. Start auto-speed function after NVF-200R reboots.
- d. NVF-800S will try to link at 25M mode with NVF-200R. If it fails, auto-speed goes down to 15M mode and re-link with NVF-200R. If it fails again, auto-speed goes down to 5M and keeps this mode then re-link with NVF-200R.
- e. Please note any length of phone cable change, NVF-200R must re-powered again due to auto-speed function work only when restarting.
- f. Await 5 ~ 120 seconds until VDSL port link up where it depends on phone cable length.

Port Controls

Port	State	Auto Negotiation	Speed	Duplex	Flow Control
1					
2	Enable	Enable	25M	Full	Enable
3					

Apply

Figure 4.69 Port Controls

Note:

VDSL port supports auto-speed mode, the speed mode depends on phone cable length and crosstalk issues, anytime auto-speed starts on, phone cable must be re-plugged and NVF-800S must be re-powered on, wait for a few minutes auto-speed to link.

- ◆ 25M/25M symmetric run up to 600 meters (without PBX)
- ◆ 15M/15M symmetric run up to 1.1km (without PBX)
- ◆ 5M/5M symmetric run up to 1.7km (without PBX)

The performance data above is for reference only, the actual distance will vary on the quality of the copper wire and environment factors. With above speed mode testing based on 24gauge twisted pair phone cable without PBX.

4.2.2.4.5 Link Aggregation

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, to move the link to that Link Aggregation Group and enable its transmission and reception functions in an orderly manner. Therefore, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, for more detail information, please refer to IEEE 802.3ad.

4.2.2.4.5.1 Aggregator setting

Trunking

Aggregator Setting		Aggregator information		State Activity	
<div>System Priority</div> <div>1</div>					
Group ID	Group1	<< Get			
Lacp	Disable				
Work Ports	0				
	<div><< Add <<</div> <div>Remove>></div>	<div>port1</div> <div>port2</div> <div>port3</div> <div>port4</div> <div>port5</div> <div>port6</div> <div>port7</div> <div>port8</div>			
<div>Apply</div> <div>Delete</div> <div>Help</div>					

Figure 4.70 Trunking(Aggregator Setting)

(Figure 4.70)

Item	Description
System Priority:	A value used to identify the active LACP. The NVF-800S with the lowest value has the highest priority and is selected as the active LACP.
Group ID:	It can create a link aggregation across two or more ports, choose the "Group ID" and click "Get".
LACP:	If enable, the group is LACP static trunking group. If disable, it is local static trunking group. All ports support LACP dynamic trunking group. If connecting to the device also supports LACP, the LACP dynamic trunking group will be created automatically.
Work ports:	The maximum number of ports can be aggregated at the same time. If LACP static trunking group, the exceed ports is standby and able to aggregate if work ports fail. If local static trunking group, the value must be the same as group ports.

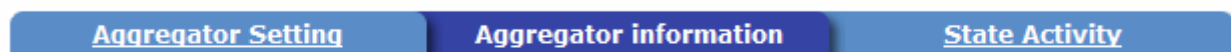
4.2.2.4.5.2 Aggregator Information

When you are setting LACP aggregator, you can see relation information in here.

Setup LACP example:

1. LACP: Enable. (One can configure LACP Active/Passive status in each port.)
2. Work ports: 2(use 2 work ports)
3. Select the ports to join the trunking group: Port1 & Port2
4. Click Apply.
5. You can see the configuration shown at the aggregator information. ([Figure 4.71](#))

Trunking



The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	1
Port_No	1 2

Figure 4.71 Trunking(Aggregator information)

4.2.2.4.5.3 State Activity

Item	Description
Active (select):	The port automatically sends LACP protocol packets.
Passive (no select):	The port does not automatically sends LACP protocol packets and responds only if it receives LACP protocol packets from the opposite device.

Tip: (Figure 4.72)

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for LACP protocol packet from the opposite device.
2. If one is an active LACP's actor, when one should select trunking port, the active status will be created automatically.

Trunking

Aggregator Setting

Aggregator information

State Activity

Port	LACP State Activity	Port	LACP State Activity
1	N/A	5	<input type="checkbox"/> Active
2	N/A	6	<input type="checkbox"/> Active
3	<input type="checkbox"/> Active	7	<input type="checkbox"/> Active
4	<input type="checkbox"/> Active	8	<input type="checkbox"/> Active

Apply

Default

Help

Figure 4.72 Trunking(State Activity)

4.2.2.4.6 Filter Database

4.2.2.4.6.1 IGMP Snooping

The NVF-800S supports IP multicast, to enable IGMP protocol on web management's NVF-800S setting advanced page, then display the IGMP snooping information in this page, it can view different multicast group, VID and member port, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

IP manages multicast traffic by using NVF-800S, bridges and hosts that support IGMP. Enabling IGMP allow the ports to detect IGMP queries and report packets and manage IP multicast traffic through the NVF-800S ([Figure 4.73](#))

IGMP Snooping
Static MAC Addresses
Port Security
MAC Filtering

Multicast Group

Ip_Address	VID	MemberPort
239.255.255.250	0009	***** 09 10

Figure 4.73 IGMP Snooping

IGMP have three fundamental types of message as follows:

Item	Description
Query:	A message sent from the queries (IGMP bridge or NVF-800S) asking for a response from each host belonging to the multicast group.
Report:	A message sent by a host to the queries to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group:	A message sent by a host to the queries to indicate that the host has quit being a member of a specific multicast group.

4.2.2.4.6.2 Static MAC Address

IGMP Snooping
Static MAC Addresses
Port Security
MAC Filtering

Static addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address
PORT

MAC Address

Port Num

Vlan ID

Figure 4.74 Static MAC Address

When you add a static MAC address, it remains in the NVF-800S address table, regardless of whether the device is physically connected to the NVF-800S. This saves the NVF-800S from having to re-learn a device MAC address when disconnected or powered off device is active on the network again. (Figure 4.74)

1. To add a static MAC address.
2. Go to main menu, click administrator then click Filter Database.
3. Click Static MAC Addresses. In the MAC address box, enter the MAC address to and from which the port should

permanently forward traffic, regardless of the device network activity.

4. In the Port Number box, select a port number.
5. If tag-based (IEEE 802.1Q) VLANs are set up on the NVF-800S, static addresses are associated with individual VLANs.
Type the VID (tag-based VLANs) associated with the MAC address.
6. Click "add"

4.2.2.4.6.3 Port Security

A port in security mode will be "locked" without permission of address learning. Only the incoming packets with Static MAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings then click apply to save the changes. (Figure 4.75)

IGMP Snooping
Static MAC Addresses
Port Security
MAC Filtering

Port	Enable Security (disable for MAC Learning)	Port	Enable Security (disable for MAC Learning)
1	<input type="checkbox"/>	6	<input type="checkbox"/>
2	<input type="checkbox"/>	7	<input type="checkbox"/>
3	<input type="checkbox"/>	8	<input type="checkbox"/>
4	<input type="checkbox"/>	9	<input type="checkbox"/>
5	<input type="checkbox"/>	10	<input type="checkbox"/>

Figure 4.75 Port Security

4.2.2.4.6.4 MAC Filtering

MAC address filtering allows the NVF-800S to drop unwanted traffic. Traffic is filtered based on the destination address. For example, if one network is congested because of high utilization from one MAC address, one can filter all traffic transmitted from that MAC address, restoring network flow while one troubleshoot the problem. (Figure 4.76)

[IGMP Snooping](#)
[Static MAC Addresses](#)
[Port Security](#)
[MAC Filtering](#)

Specify a MAC address to filter.

MAC Address

Mac Address

Vlan ID

N/A

Add

Delete

Help

Figure 4.76 MAC Filtering

4.2.2.4.7 VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows one to isolate network traffic so only members of the VLAN can receive traffic from the same VLAN members. Basically, creating a VLAN from a NVF-800S is a logically equivalent of reconnecting a group of network devices to another Layer 2 NVF-800S. However, all the network devices are still plug into the same NVF-800S physically.

The NVF-800S supports port-based and protocol-based VLAN in web management. In the default configuration, VLAN is enabled and all ports on the NVF-800S belong to default VLAN, VID is 1.

Support Multiple VLAN (IEEE 802.1Q VLAN)

Port-based tagging rule VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different NVF-800S vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

Support Protocol-based VLAN

In order for an end station to send packets to different VLAN, it has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

NVF-800S will support protocol-based VLAN classification by means of both built-in knowledge of layer 2 packet formats used by selected popular protocols such as Novell IPX and AppleTalk's EtherTalk and some degree of programmable protocol matching capability. (Figure 4.77)

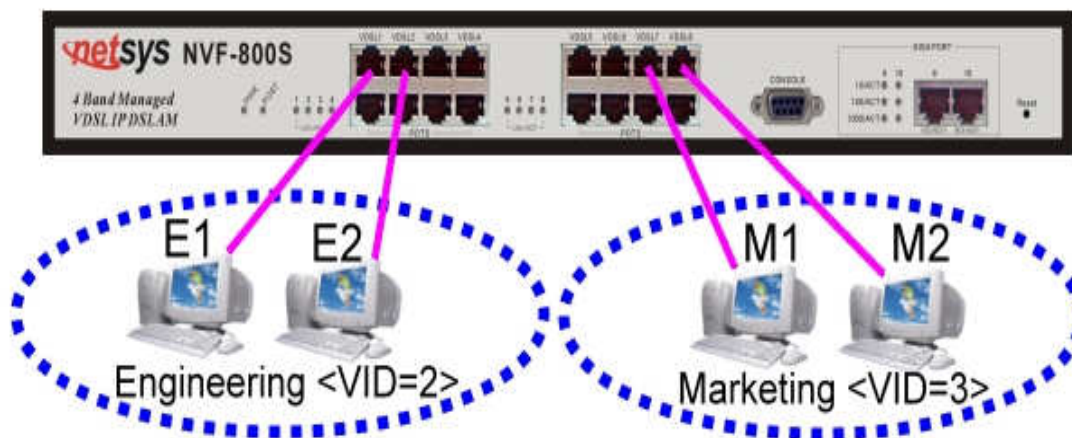


Figure 4.77 VLAN connection diagram

4.2.2.4.7.1 Basic

Tag-based (IEEE 802.1Q) VLAN

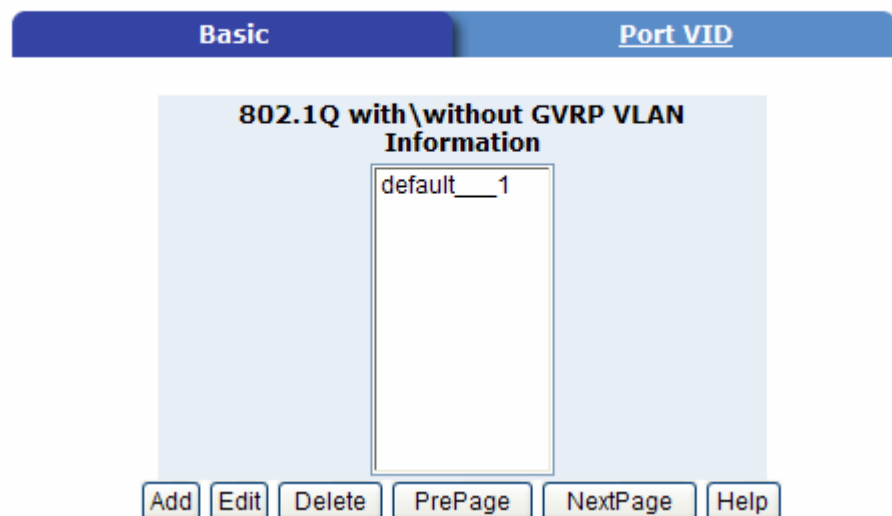


Figure 4.78 802.1Q VLAN Basic

For Example, create a VLAN and add tagged members in it. (Figure 4.78)

1. From the main menu, click administrator → VLAN configuration.
2. Click “Add”.
3. Type a name for the new VLAN.
4. Type a VID (between 2~4094), where the default is 1.
5. From the available ports box, select ports to add to the NVF-800S and click “Add”.
6. Click “Apply”.

4.2.2.4.7.2 Port VID

Tag-based (IEEE 802.1Q) VLAN

Basic
Port VID

Assign a Port VLAN ID (1~4094) for untagged traffic on each port, then click Submit to apply the changes on this page.

No.	PVID	Ingress Filtering 1	Ingress Filtering 2	No	PVID	Ingress Filtering 1	Ingress Filtering 2
1	1	Enable ▾	Disable ▾	6	1	Enable ▾	Disable ▾
2	1	Enable ▾	Disable ▾	7	1	Enable ▾	Disable ▾
3	1	Enable ▾	Disable ▾	8	1	Enable ▾	Disable ▾
4	1	Enable ▾	Disable ▾	9	1	Enable ▾	Disable ▾
5	1	Enable ▾	Disable ▾	10	1	Enable ▾	Disable ▾

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

Apply Default Help

Figure 4.79 802.1Q VLAN Port VID

Configure Port VID setting (Figure 4.79)

From the main Tag-based (IEEE 802.1Q) VLAN page, click Port VID Settings.

Port VID (PVID)

Set the Port VLAN ID that will be assigned to untagged traffic on a given port. For example, if port 10's default PVID is 100, all untagged packets on port 10 will belong to VLAN 100. The default setting for all ports is VID 1.

This feature is useful for accommodating devices that one wants to participate in the VLAN but don't support tagging. Only one untagged VLAN is allowed per port.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.

NVF-800S has two ingress filtering rule:

Ingress Filtering **Rule 1**: Forward only packets with VID matching this port's configured VID.

Ingress Filtering **Rule 2**: Drop Untagged Frame.

4.2.2.4.8 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in NVF-800S networks. When STP is enabled, it ensures that only one path is active at a time between any two nodes on the network. (Figure 4.80)

1. The following parameter can be configured on each port, click Apply button to modify.

Configure Spanning Tree Port Parameters

Port Number	Priority (0 - 255; Default 128)	Path Cost (1 - 65535; Default 10)
<div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> </div>	128	10

Figure 4.80 Spanning Tree port parameters

Item	Description
Port Priority:	To make it more or less likely to become the root port, the range is 0~255, where default setting is 128. The lowest number has the highest priority. If the value is changed, NVF-800S must be rebooted.
Path Cost:	Specify the path cost of the port that NVF-800S uses to determine which port are the forwarding ports. The lowest number is forwarding ports, the range is 1~65535 and default value based on IEEE802.1D 10Mbps = 50~600 100Mb/s = 10~60 1000Mb/s = 3~10. If the value is changed, NVF-800S must be rebooted.

2. Spanning tree information can be viewed at the Root Bridge: (Figure 4.81)

Root Bridge Information	
Priority	32768
Mac Address	00056e002557
Root_Path_Cost	20
Root Port	10
Max Age	20
Hello Time	2
Forward Delay	15

Figure 4.81 Root Bridge Information

3. STP parameter can be set at the Configure Spanning Tree Parameters, click Apply button to modify. (Figure 4.82)

Configure Spanning Tree Parameters	
Priority (1-65535)	<input type="text" value="32768"/>
Max Age (6-40)	<input type="text" value="15"/>
Hello Time (1-10)	<input type="text" value="2"/>
Forward_Delay_Time(4-30)	<input type="text" value="5"/>

Figure 4.82 Configure Spanning tree parameters

Item	Description
Priority:	To change priority value. A value must be used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Value ranges from 1 to 65535.
Max Age:	To change Max Age value. The number of seconds a bridge waits without receiving. Spanning Tree Protocol configuration messages before attempting a reconfiguration. Value ranges from 6 to 40.
Hello Time:	To change Hello time value. The number of seconds between the transmit time of Spanning Tree Protocol configuration messages. Value ranges from 1 to 10.
Forward Delay time:	To change forward delay time. The number of seconds a port waits before changing from its Spanning Tree Protocol learning and listening states to the forwarding state. Value ranges from 4 to 30.

4. Spanning tree status can be viewed at the NVF-800S STP Port Status. (Figure 4.83)

STP Port Status			
PortNum	PathCost	Priority	PortState
1	10	128	DISABLED
2	10	128	DISABLED
3	10	128	DISABLED
4	10	128	DISABLED
5	10	128	DISABLED
6	10	128	DISABLED
7	10	128	DISABLED
8	10	128	DISABLED
9	10	128	FORWARDING
10	10	128	FORWARDING

Figure 4.83 STP port status

4.2.2.4.9 Port Sniffer

The Port Sniffer is a method for monitoring traffic in NVF-800S networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into sniffer port. (Figure 4.84)

Item	Description
Roving Analysis State:	Enable or disable the port sniffer function.
Analysis Port:	Analysis port can be used to see all monitor port traffic. It can connect sniffer port to LAN Analysis, Session Wall or Netxray.
Monitor Ports:	The ports one wants to monitor. All monitor port traffic will be copied to sniffer port. You can select maximum of 9 monitor ports in the NVF-800S. If one wants to disable the function, one must select monitor port to none.
Monitor Rx:	Monitor received frames from the port.
Monitor Tx:	Monitor sent frames from the port.

Port Sniffer

Roving Analysis State: DISABLE		
Analysis Port: None		
Monitor Ports	Monitor Rx	Monitor Tx
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
Apply	Default	Help

Figure 4.84 Port Sniffer

4.2.2.4.10 SNMP

Any Network Management running the Simple Network Management Protocol (SNMP) can manage the NVF-800S provided that the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a protocol that governs the transfer of information between management and agent. The VDSL NVF-800S support SNMP V1.

1. Use this page to define management stations as trap managers and enter SNMP community strings. User can also define a name, location and contact person for the NVF-800S. Fill in the system options data then click Apply to update the changes on this page. ([Figure 4.85](#))

Item	Description
Name:	Enter a name to be used for the NVF-800S.
Location:	Enter the location of the NVF-800S.
Contact:	Enter the name of a person or organization.

SNMP Management

System Options

Name :

Location :

Contact :

Figure 4.85 SNMP Management

2. Community strings serve as passwords and can be entered as one of the following: (Figure 4.86)

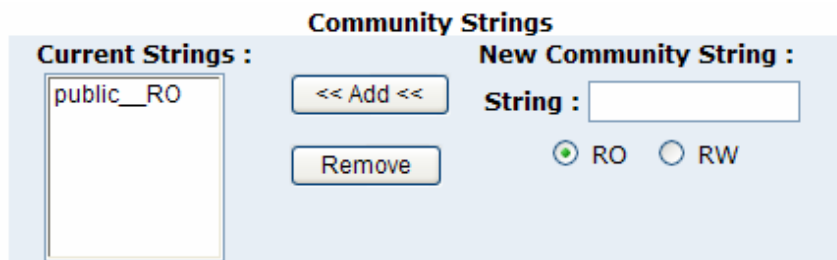


Figure 4.86 SNMP Community Strings

Read only: Enables requests accompanied by this string to display MIB-object information.

Read write: Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

3. Trap Manager

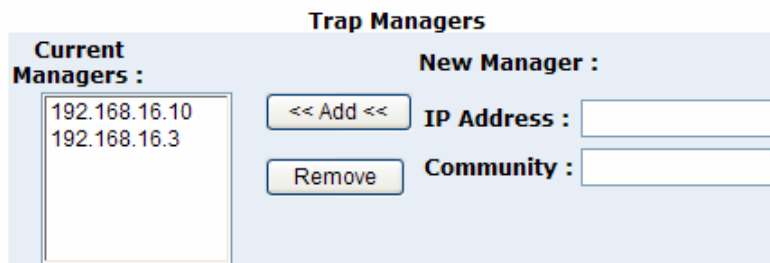


Figure 4.87 SNMP Trap Managers

A trap manager is a management station that receives traps and system alerts generated by the NVF-800S. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string. (Figure 4.87)

Enterprise MIB contains two traps:

- When NVF-800S internal temperature is greater than 70°C, system will send a "Temperature alarm" trap.
- When the NVF-800S internal cooling FAN doesn't run, the system will send a "FAN speed alarm" trap.

4.2.2.4.11 Interleave

This function is used in digital data transmission technology to protect the transmission against noise issue and data error.

If during transit more than a certain amount of data has been lost then the data cannot be correctly decoded. Short bursts of noise on the line can cause these data packets to become corrupt and the bridge has to re-request data which in turn can slow down the overall rate at which data is transmitted.

Interleaving is a method of taking data packets, chopping them up into smaller bits and then rearranging them so that once contiguous data is now spaced further apart into a non continuous stream. Data packets are re-assembled by your bridge.

The diagram below is an example of how interleaved traffic is transmitted. (Figure 4.88)

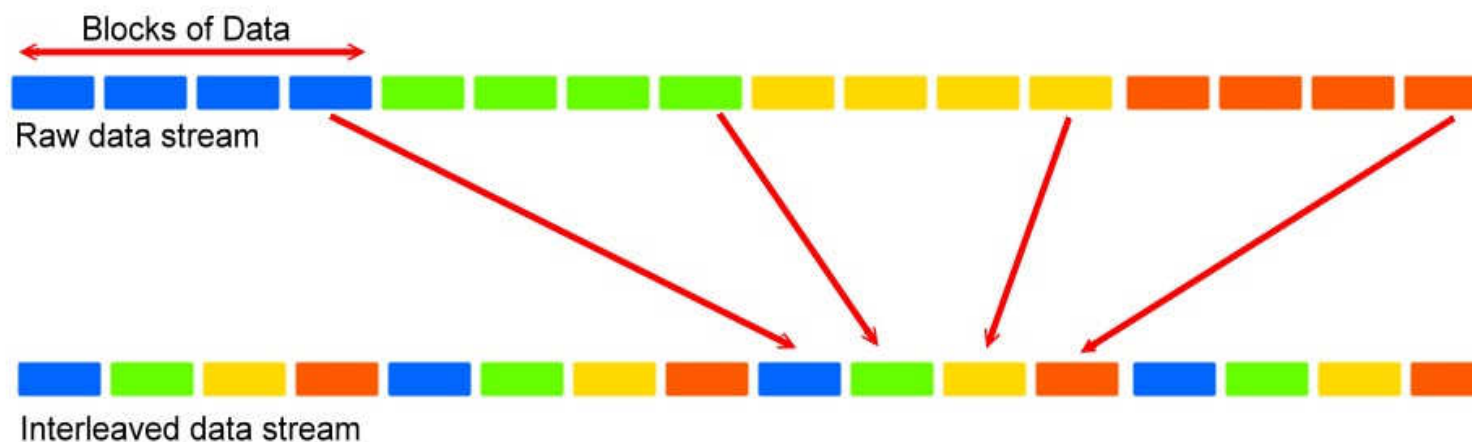


Figure 4.88 Interleave diagram

If your line is particularly susceptible to bursts of noise then interleaving should improve your vdsl experience simply because if you lose a whole batch of data then this could cause your bridge to loose sync with the exchange.

Using Interleaving, the bridge is able to re-assemble the data or if necessary just re-request the part of the data that it is unable to recover. By increasing the interleave depth of each ports that are susceptible to noise, this will improve error performance and stability of marginal lines.

Interleave Depth is defines as the number of bits (or bytes) in each block of data.

VDSL supports a various levels of interleaving, the depth of which can range from 0 (no interleaving) to 64.

Interleave Delay applies only to the interleave channel and defines the mapping (relative spacing) between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.

Maximum Interleave Delay is the configurable attribute on some DSLAMs/bridges as the maximum time for the Interleave Delay. The higher the Interleave Delay the greater the Interleaving Depth. In this field, enter the value for the Downstream/Upstream Parameter, Configured maximum Interleave Delay, for this channel.

Note:

Interleaving Depth & Interleaving Delay do not appear to be the same thing as the additional amount of latency you will see when interleaving is switched on nor is latency affected by speed (e.g. it does not decrease when one go from 1Mbits to 5Mbits).

The following ports can modify the desired interleave depth. (Figure 4.89)

Interleaver depths

Port	Interleave Depth
<div> <div>6</div> <div>7</div> <div>8</div> </div>	<div>0</div>

Apply

Figure 4.89 Interleaver depth

The current information provides a view of the current status of the unit.

Interleave depth value will show in the status only if the port is connected. (Figure 4.90)

Port	Interleave Depth	
	Config	Status
1	16	16
2	8	0
3	8	0
4	8	0
5	8	0
6	8	0
7	8	0
8	8	0

Figure 4.90 Interleaver depth config / status

4.2.2.4.12 SNR

SNR (Signal to Noise Ratio) status provides a view of the current VDSL Attenuation value of the unit. (Figure 4.91)

SNR Status

The following information provides a view of the current VDSL Attenuation value of the unit.

SNR (Signal to Noise Ratio)

Port Num	SNR	
	Value	unit
1	No Link	db
2	No Link	db
3	No Link	db
4	No Link	db
5	No Link	db
6	No Link	db
7	No Link	db
8	No Link	db

Figure 4.91 SNR Status

4.2.2.4.13 Security Manager

Security manager provides the user to change user name and password at the web management. (Figure 4.92)

Default User Name: Admin and Password: 123

Security Manager

User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="..."/>
Reconfirm password:	<input type="password" value="..."/>
<input type="button" value="Apply"/>	

Figure 4.92 Security Manager

4.2.2.4.14 TFTP Update Firmware

TFTP Update Firmware provides the system control functions to allow a user to update firmware and remotely boot the NVF-800S system. (Figure 4.93)

1. Install TFTP Server and execute the program.
2. Copy firmware update version image.bin to TFTP Server directory.
3. In the web management select administrator then go to TFTP update firmware.
4. Download new image".bin" file then in web management click apply and confirm yes to start updating firmware.

TFTP Download New Image

TFTP Server IP Address	<input type="text" value="192.168.16.12"/>
Firmware File Name	<input type="text" value="image.bin"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 4.93 TFTP Download New Image

4.2.2.4.15 Configuration Backup

4.2.2.4.15.1 TFTP Restore Configuration

Use this page to set TFTP server IP Address and Restore File Name. To restore EEPROM value, put back flash.dat file in TFTP server and the NVF-800S will download back the flash image. ([Figure 4.94](#))

TFTP Configuration

TFTP Restore Configuration		TFTP Backup Configuration
TFTP Server IP Address	<input type="text" value="192.168.16.12"/>	
Restore File Name	<input type="text" value="flash.dat"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Figure 4.94 TFTP Restore Configuraiton

4.2.2.4.15.2 TFTP Backup Configuration

Use this page to set TFTP Server IP Address and Backup File Name. To save current EEPROM value, go to the TFTP backup configuration page to backup the EEPROM value. ([Figure 4.95](#))

TFTP Configuration

TFTP Restore Configuration	TFTP Backup Configuration	
TFTP Server IP Address	<input type="text" value="192.168.16.12"/>	
Backup File Name	<input type="text" value="flash.dat"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Figure 4.95 TFTP Backup Configuration

4.2.2.4.16 Reset System

Reset NVF-800S to default configuration([Figure 4.96](#))

Reset System

Reset Switch to Default Configuration

reset

Figure 4.96 Reset system to default

Note:

Please make sure the NVF-800S has been disconnected with VDSL Bridge.

4.2.2.4.17 Reboot

Reboot the NVF-800S in software reset([Figure 4.97](#))

Reboot Switch System

reboot Help

Figure 4.97 Reboot Switch System

Chapter 5. Applications

The VDSL provides home network architecture. Transforming an apartment into a multiple home network area, sharing a single internet account for multiple users via Bridge, it can provide unlimited access time in the internet at a reasonable low price.

Bridging Functions – The NVF-800S provides full transparent bridging function that automatically connects node addresses that are later used to filter and forward all traffic based on the destination address. When traffic passes between devices attached to the shared collision domain, those packets are filtered from the NVF-800S. But when traffic must be passed between unique segments (e.g. different ports of the NVF-800S), a temporary link is set up between the NVF-800S port in order to pass this traffic.

Transceiver function

The NVF-800S support Ethernet to VDSL converter, it can be transmit or receive packet from Ethernet port to the RJ11 port or VDSL port to Ethernet port.

Flexible Configuration—The NVF-800S is not only designed to segment the network, but also to provide a wide range of options in the configuration of home network connections. It can be used as a simple stand alone NVF-800S or can be connected with another IP DSLAM, Bridge, XDSL, ISDN, gateway or other network interconnection devices in various configurations. Some of the common applications of the NVF-800S are described below.

Application for Video on demand and Video conference(Figure 5.1)

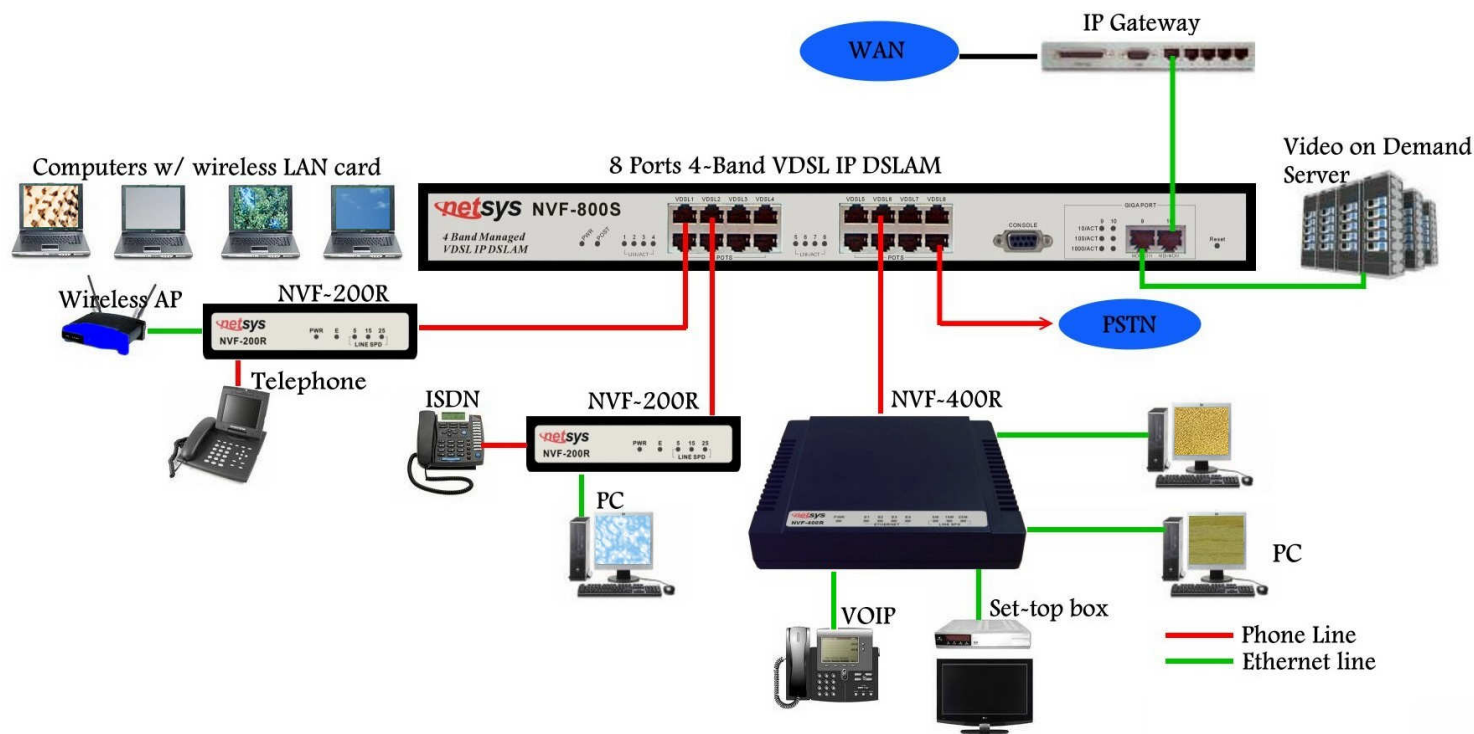
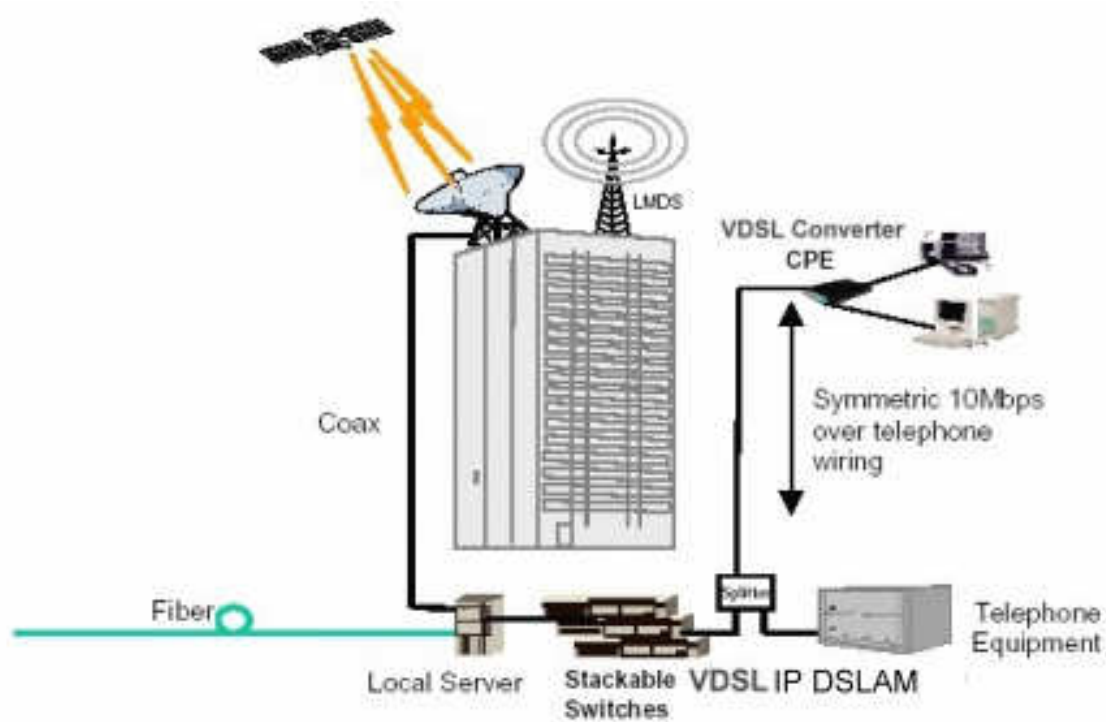


Figure 5.1 NVF-800S Application Diagram

Used as apartment for Internet access

The NVF-800S provides a high speed, auto-speed transmission over existing home telephone wiring over a single Internet account to provide simultaneous independent Internet access to multiple users.

No matter ISDN telephone system nor POTS telephone system one have, the VDSL technology let use of the telephone system and VDSL network system in the same time. (Figure 5.2)



Broadband Access Applications Utilizing VDSL IP DSLAM

Figure 5.2 NVF-800S Application Diagram-2

Application for sharing a single internet account

If multiple users would like to share a single internet account using the NVF-800S which is to be connected to an IP sharing device then connected to xDSL. (Figure 5.3)

Note:

For network applications that actually require Bridge (e.g. Interconnecting dissimilar network types), attaching the NVF-800S directly to a bridge can significantly improve overall home networking performance.

High bandwidth backbone ready

The NVF-800S provides 10/100/1000Mbps auto sensing for external trunk device (Fiber optics, Wireless Router, xDSL & other WAN services)

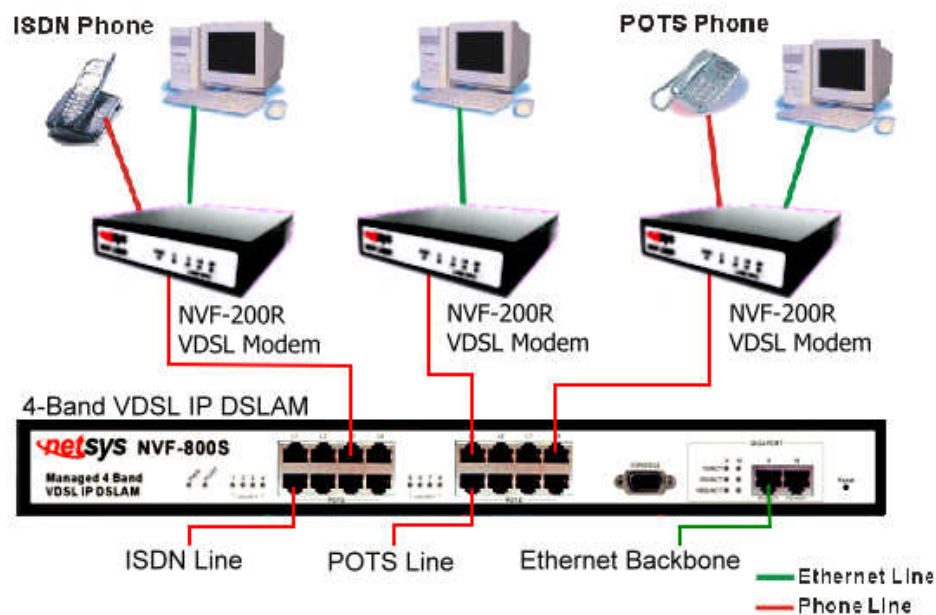


Figure 5.3 NVF-800S Application Diagram-3

Appendix A: Cable Requirements

A.1 Ethernet Cable

A CAT 3, 4 or 5 UTP (unshielded twisted pair) cable is typically used to connect the Ethernet device to the modem. A 10Base-T cable often consists of four pairs of wires, two of which are used for transmission. The connector at the end of the 10Base-T cable is referred to as an RJ-45 connector and it consists of eight pins. The Ethernet standard uses pins 1, 2, 3 and 6 for data transmission purposes. ([Table A-1](#))

Table A-1 RJ-45 Ethernet Connector Pin Assignments

PIN #	MDI		MDI-X	
	Signal	Media Dependant interface	Signal	Media Dependant interface-cross
1	TX+	Transmit Data +	RX+	Receive Data +
2	TX-	Transmit Data -	RX-	Receive Data -
3	RX+	Receive Data +	TX+	Transmit Data +
4	--	Unused	--	Unused
5	--	Unused	--	Unused
6	RX-	Receive Data -	TX-	Transmit Data -
7	--	Unused	--	Unused
8	--	Unused	--	Unused

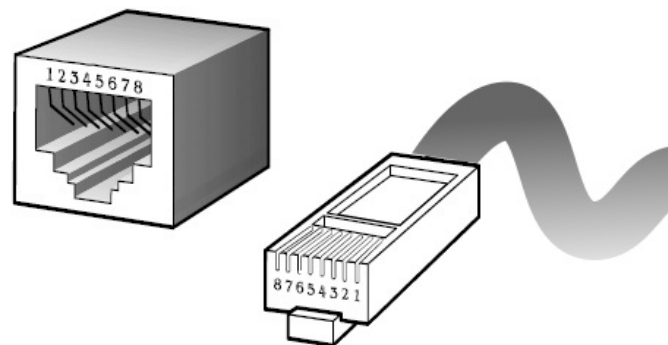


Figure A-1 Standard RJ-45 repectacle/connector

Note:

Please make sure your connected cables are with same pin assignment as above table before deploying the cables into your network.

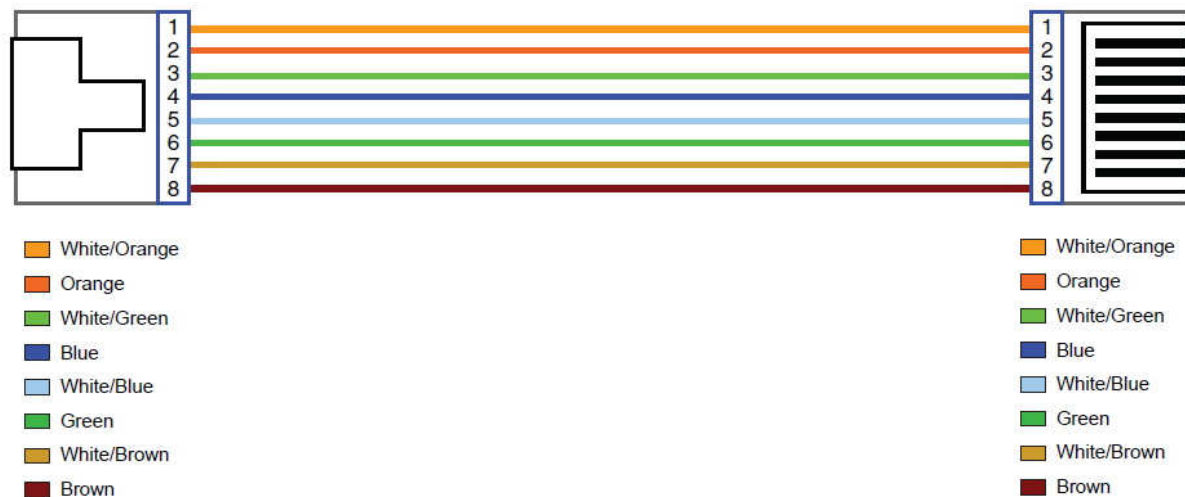


Figure A-2 Pin Assignments and Wiring for an RJ-45 Straight-Through Cable

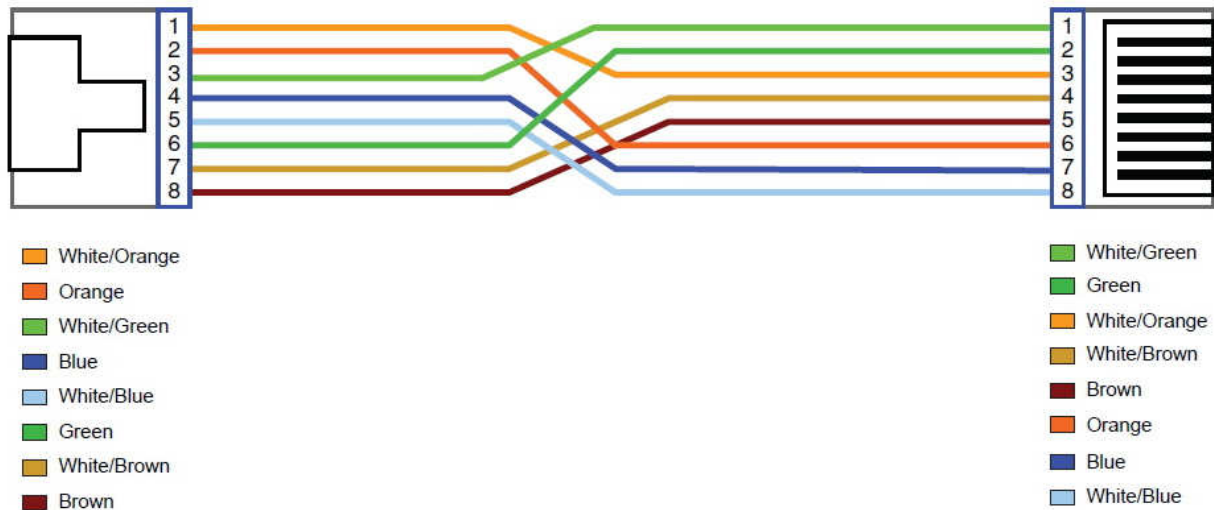


Figure A-3 Pin Assignments and Wiring for an RJ-45 Crossover Cable

A.2 Telephone wire

Standard telephone wire of any gauge or type-flat, twisted or quad is used to connect the Modem to the telephone network. A telephone cable typically consists of three pairs of wires, one of which is used for transmission. The connector at the end of the telephone cable is called an RJ-11 connector and it consists of six pins. POTS (plain old telephone services) use pins 3 and 4 for voice transmission. A telephone cable is shown below. (Figure A-4)

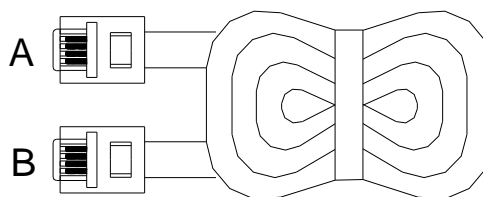


Figure A-4 Telephone cable

The A and B connectors on the rear of the Modem are RJ-11 connectors. These connectors are wired identically. The RJ-11 connectors have six positions, two of which are wired. The Modem uses the center two pins. The pin out assignment for these connectors is presented below. (Table A-2)

Table A-2 RJ-11 Pin out Assignments

Pin#	MNEMONIC	FUNCTION
1	NC	Unused
2	NC	Unused
3	TIP	POTS
4	RING	POTS
5	NC	Unused
6	NC	Unused_

A.3 Serial Console Interface Connector Pin Assignments

The serial console interface connector is a 9-pin, RS-232 D-type, DTE connector. A null modem cable is required to connect a workstation running the Linux or Windows operating system. Table A-3 lists the pin assignments for the serial console interface connector.

Table A-3 RS-232 Connector Pin Assignments

Description	Pin	I/O	Signal Name
Not used	1	-	-
Receive data; input	2	In	RXD
Transmit data; output	3	Out	TXD
Data terminal ready; output	4	Out	DTR
Interface signal ground	5	-	GND
Data set ready; input	6	In	DSR
Not used	7	-	-
Not used	8	-	-
Not used	9	-	-

The CDEs have one standard serial port connector located on the back of the device. Figure A-5 shows the pin number assignments for the 9-pin, male D-shell serial port connector on the back of the device. These pin number assignments conform to the industry standard for RS-232 communications.

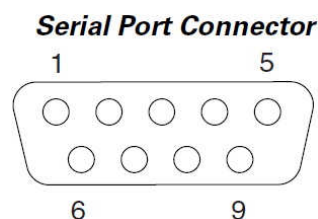


Figure A-5

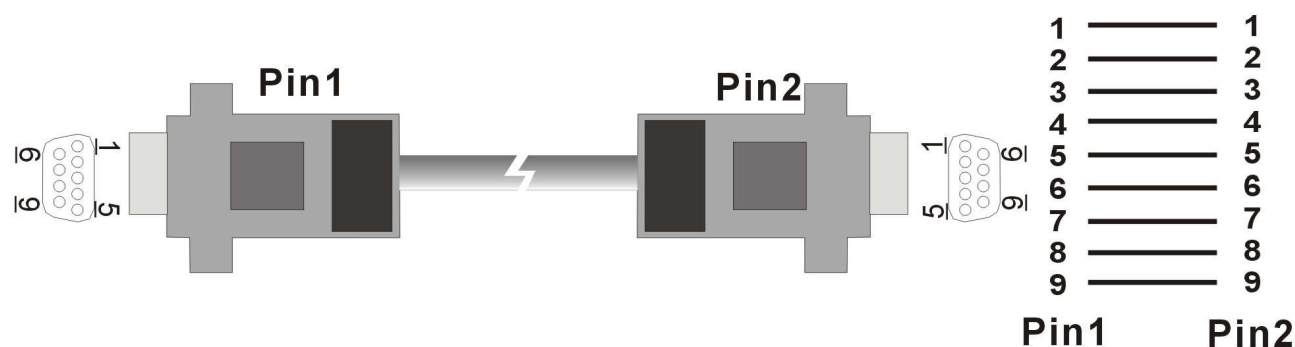


Figure A-6 Pin Assignments and Wiring for an RS-232 Cable

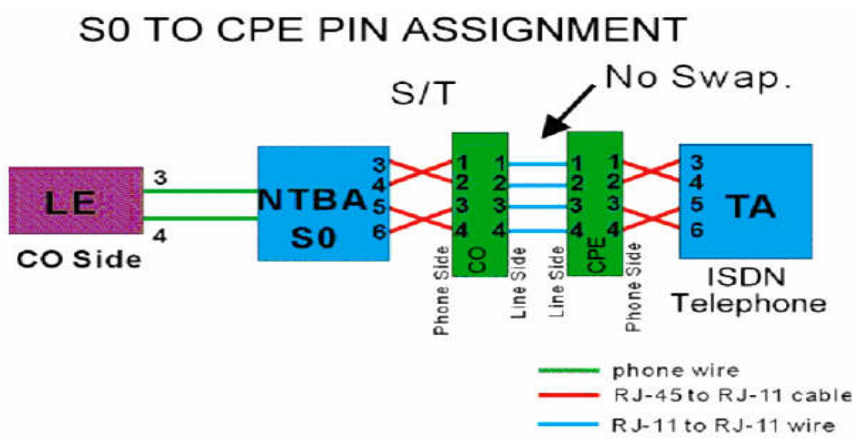
Appendix B: Troubleshooting

Diagnosing VDSL Indicators

The VDSL can be easily monitored through its comprehensive panel indicators. These indicators assist the network manager in identifying problems the NVF-800S may encounter. This section describes common problems you may encounter and possible solutions

1. Symptom:	POWER indicator does not light up (green) after power on.
Cause:	Defective power outlet, power cord, internal power supply
Solution:	Cheek the power outlet by trying another outlet that is functioning properly. Check the power cord with another device. If these measures fail to resolve the problem, have the unit power supply replaced by a qualified distributor.
2. Symptom:	Link indicator does not light up (green) after making a connection.
Cause:	Network interface (e.g. a network adapter card on the attached device), network cable, or NVF-800S port is defective).
Solution:	<ul style="list-style-type: none"> ◆ Verifies the NVF-800S and attached device are powered on. ◆ Be sure the cable is plug into both the NVF-800S and corresponding device. ◆ Verify that the proper cable type is used and its length does not exceed specified limits. ◆ Check the adapter on the attached device and cable connections for possible defects. ◆ Replace the defective adapter or cable if necessary.
3. Symptom:	VDSL always link on 5M/5M speed mode at short phone cable.
Cause:	VDSL auto speed lock up.
Solution:	Please re-power NVF-200R.
Note:	NVF-800S will redo auto speed function while NVF-200R re-power on.

4. Symptom:	VDSL link cannot be established.
Cause:	VDSL speed mode setting failure or phone cable length is over the specification limit of the speed mode.
Solution:	<ul style="list-style-type: none"> ◆ Please make sure that the phone wire must be connected between NVF-800S and VDSL CPE Modem when both are power on. NVF-800S will do link speed function depending on speed mode setting and phone wire length, therefore if NVF-800S can't detect VDSL CPE Modem over phone wire while both power on, this will cause the link to fail. ◆ Please check phone cable must be 24 gauge with twisted pair and without rust, and the length is not over 1.9km.
Note:	Phone cable must meet CAT 3 standard or above and without clustering, otherwise will cause more cross talk issue to reduce DSL power driver.

5. Symptom:	We tested with a regular S0 bus from an NTBA - data works, but ISDN telephone does not.
Solution:	<p>You must connect according to the following chart if you want to connect CO and CPE with NTBA.</p> <p style="text-align: center;">S0 TO CPE PIN ASSIGNMENT</p>  <p>The diagram illustrates the pin assignment for connecting an S0 bus from an NTBA to an ISDN telephone. It shows the following components and their connections:</p> <ul style="list-style-type: none"> LE (CO Side): A purple box with pins 3 and 4. NTBA S0: A blue box with pins 3, 4, 5, and 6. Phone Side CO: A green box with pins 1, 2, 3, and 4. Line Side CPE: A green box with pins 1, 2, 3, and 4. TA (ISDN Telephone): A blue box with pins 3, 4, 5, and 6. <p>Connections are as follows:</p> <ul style="list-style-type: none"> LE pin 3 to NTBA S0 pin 3 (green line). LE pin 4 to NTBA S0 pin 4 (green line). NTBA S0 pin 3 to Phone Side CO pin 1 (red line). NTBA S0 pin 4 to Phone Side CO pin 2 (red line). NTBA S0 pin 5 to Phone Side CO pin 3 (red line). NTBA S0 pin 6 to Phone Side CO pin 4 (red line). Phone Side CO pin 1 to Line Side CPE pin 1 (blue line). Phone Side CO pin 2 to Line Side CPE pin 2 (blue line). Phone Side CO pin 3 to Line Side CPE pin 3 (blue line). Phone Side CO pin 4 to Line Side CPE pin 4 (blue line). Line Side CPE pin 1 to TA pin 3 (blue line). Line Side CPE pin 2 to TA pin 4 (blue line). Line Side CPE pin 3 to TA pin 5 (blue line). Line Side CPE pin 4 to TA pin 6 (blue line). <p>Legend:</p> <ul style="list-style-type: none"> Green line: phone wire Red line: RJ-45 to RJ-11 cable Blue line: RJ-11 to RJ-11 wire <p>An arrow points to the Line Side CPE box with the text "No Swap."</p>

6. Symptom:	VDSL line is at link margin.
Cause:	When the VDSL line is linking between 2 speeds at 5/15Mbps or 15/25Mbps.
Solution:	Fixed the speed to 5Mbps when it is linking between 5/15Mbps or fixed the speed to 15Mbps when it is linking between 15/25Mbps.
7. Symptom:	VDSL flickers at 25Mbps when multicast streams.
Cause:	Power level is too high and noise immunity is weak.
Solution:	Fixed the speed to 15Mbps since 15Mbps is ideal for multicast streaming while 25Mbps is for transferring large data file at high speed.

System Diagnostics

Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply as explained in the previous section. However, if the unit should turn itself off after running for a while, check for loose power connections, power loss or surges at the power outlet, and verify that the fan on back of the unit is unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective. In this case, contact your supplier for assistance.

Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g. the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

Transmission Mode

The selections of the transmission mode for the RJ-45 ports are auto-negotiation using the default method. Therefore, if the Link signal is disrupted (e.g., by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of industry-standard connection policy, if you are using a full-duplex device that does not support auto-negotiation, communications can be easily lost (i.e., reset to the wrong mode) whenever the attached device is reset or experiences a power fluctuation. The best way to resolve this problem is to upgrade these devices to version that will support auto-negotiation.

Cabling

1. Verify that the cable type is correct. Be sure RJ-45 cable connectors are securely seated in the required ports. Use 100Ω straight-through cables for all standard connections. Use Category 5 cable for 100/1000Mbps Fast Ethernet connections, or Category 3, 4 or 5 cables for standard 10Mbps Ethernet connections. Be sure RJ-45 phone wiring, use **18~26 gauge**.
2. Make sure all devices are connected to the network. Equipment any have been unintentionally disconnected from the network.
3. When cascading two devices using RJ-45 station ports at both ends of the cable (i.e. not an MDI port), make sure a crossover cable is used. Crossover cable should only be used if a MDI port is not available.

Physical Configuration

If problems occur after altering the network configuration, restore the original connections, and try to track the problem down by implementing the new changes, one step at a time. Ensure that cable distances and other physical aspects of the installation do not exceed recommendations

System Integrity

As a last resort verify the NVF-800S integrity with a power-on reset. Turn the power to the NVF-800S off and then on several times. If the problem still persists and you have completed all the preceding diagnoses, contact your dealer for assistance.

Appendix C: VDSL Spectrum

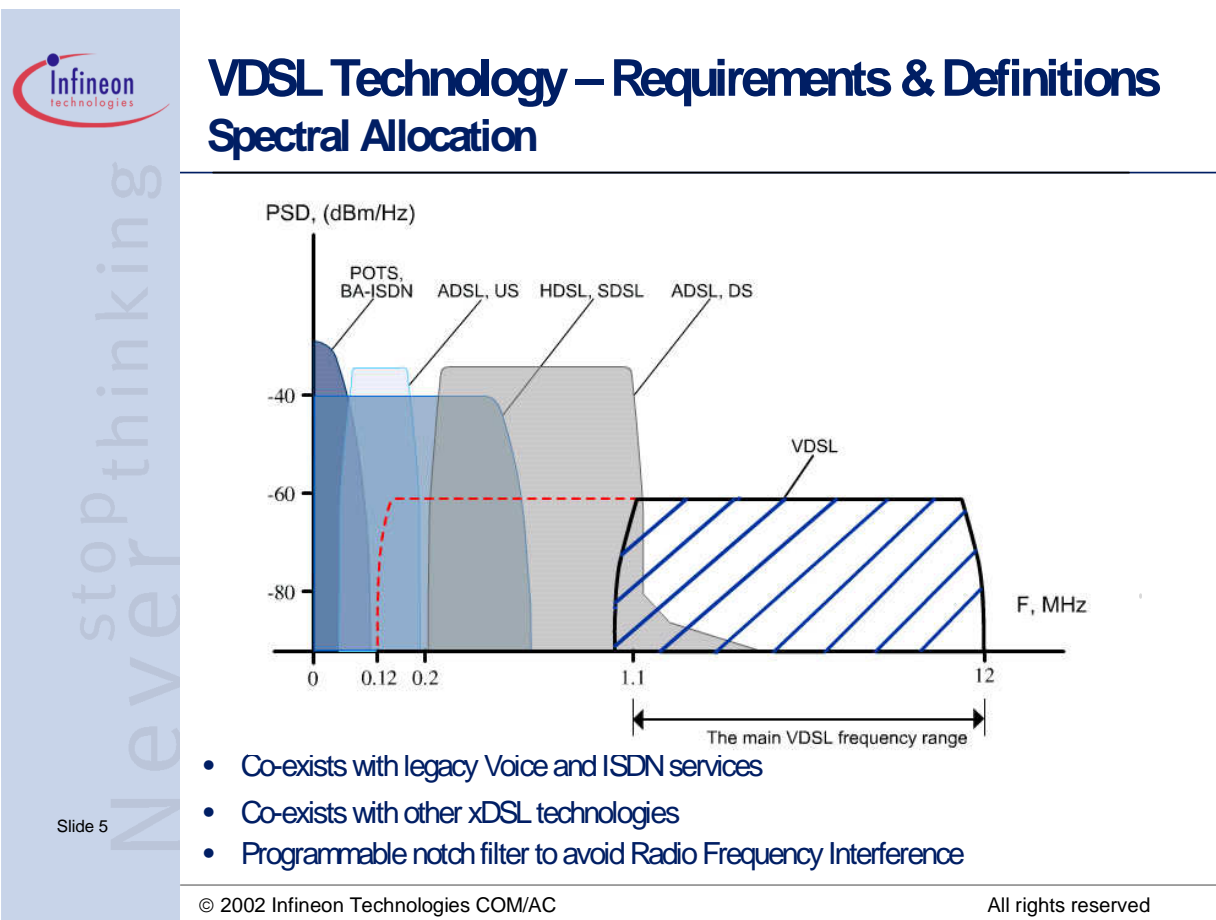


Figure C.1 VDSL Spectral Allocation

Appendix D: 4 Band VDSL Electrical Characteristics

Parameter		Min.	Typ.	Max.	Unit
Spectrum	Transmit	0.9	-	3.9	MHz
	Receive	4	-	7.9	MHz
PSD Level	Transmit	-70	-	-61.5	dBm/Hz
	Receive	-70	-	-60	dBm/Hz
Noise Margin		-	6	-	dB
5Mbps Link Margin	Transmit	27	31	35	dB
	Receive	27	31	35	dB
15Mbps Link Margin	Transmit	36	38	40	dB
	Receive	36	38	40	dB
25Mbps Link Margin	Transmit	41	43	45	dB
	Receive	41	43	45	dB

Appendix E: Examples of VLAN Setting

1. Port_Based VLAN Setting

Web management → Administrator → NVF-800S settings → Advanced:

Protocol Enable Setting → VLAN Operation Mode: Select “**Port_Based**” (Figure E-1)

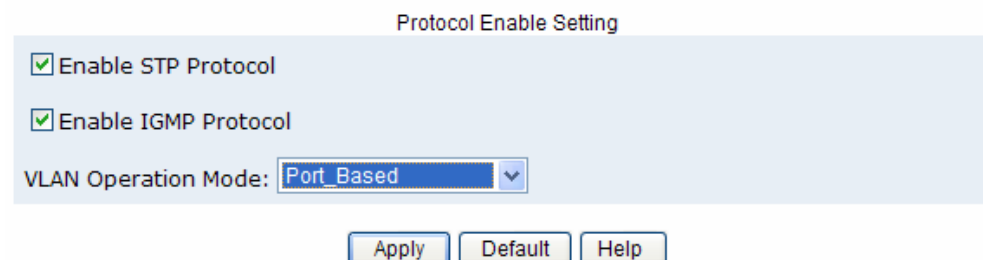


Figure E.1 Select Port_Based

Web management → Administrator → NVF-800S settings → VLAN Configuration: (Figure E-2)

Port based VLAN

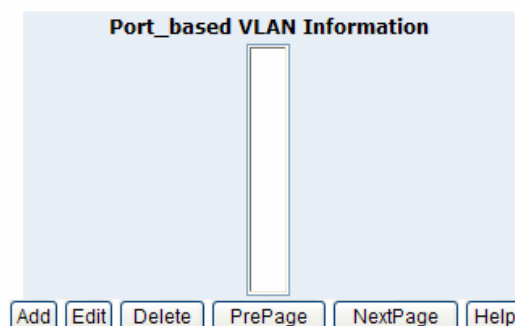
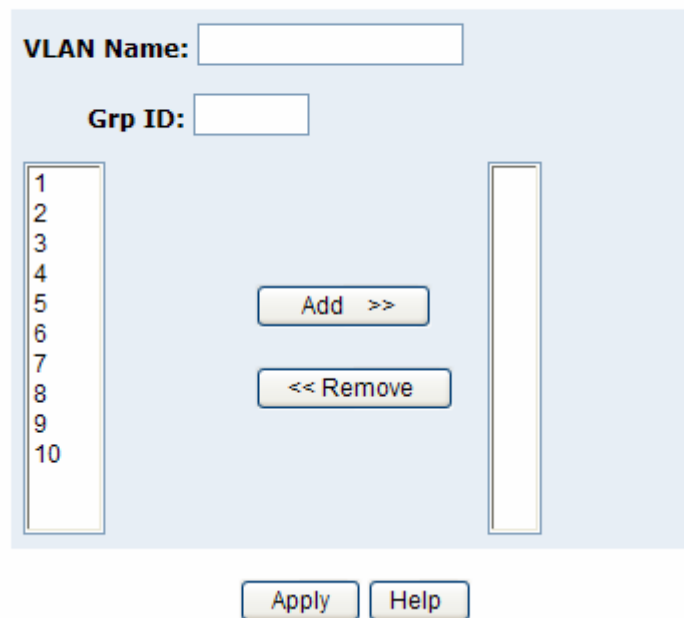


Figure E.2 Port_based VLAN Information

Add VLAN Group 1, member: port 1 and port 9. (Figure E-3)

Port based VLAN



VLAN Name:

Grp ID:

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Add >>

<< Remove

Apply Help

Figure E.3 Add VLAN group

2. Tag-Based (IEEE 802.1Q) VLAN Setting

Web management → Administrator → NVF-800S settings → Advanced:

Protocol Enable Setting → VLAN Operation Mode: Select “**802.1Q without GVRP**” ([Figure E-4](#))

Protocol Enable Setting

☒ Enable STP Protocol

☒ Enable IGMP Protocol

VLAN Operation Mode: 802.1Q without GVRP ▼

Apply
Default
Help

Figure E.4 Select “802.1Q without GVRP”

Administrator → VLAN Configuration: Select **"Port VID"** in this stage, you can define each port's PVID and set traffic rules for each port. (Figure E-5)

Note: There are two basic rules for setting traffic filtering rule while you use Tag VLAN.

1. Ingress rule will be taking effect when the packet is "incoming" packet.
2. Ingress rule 1 and 2 will be checked when you use tag. Otherwise the ingress rule will be meaningless.

Tag-based (IEEE 802.1Q) VLAN

Basic
Port VID

Assign a Port VLAN ID (1~4094) for untagged traffic on each port, then click Submit to apply the changes on this page.

No.	PVID	Ingress Filtering 1	Ingress Filtering 2	No.	PVID	Ingress Filtering 1	Ingress Filtering 2
1	1	Enable ▼	Disable ▼	6	1	Enable ▼	Disable ▼
2	1	Enable ▼	Disable ▼	7	1	Enable ▼	Disable ▼
3	1	Enable ▼	Disable ▼	8	1	Enable ▼	Disable ▼
4	1	Enable ▼	Disable ▼	9	1	Enable ▼	Disable ▼
5	1	Enable ▼	Disable ▼	10	1	Enable ▼	Disable ▼

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

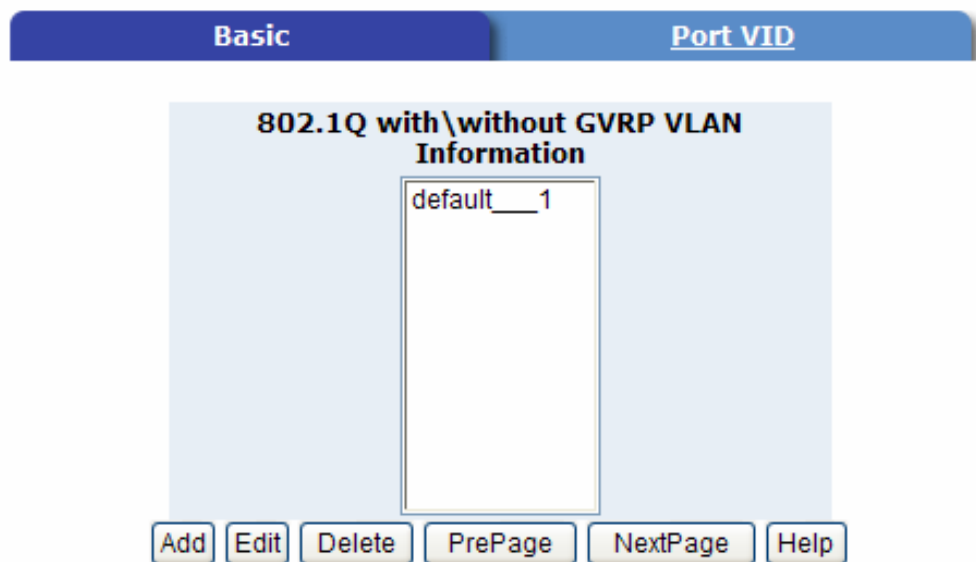
Apply
Default
Help

Figure E.5 Ingress Filtering 1 & Filtering 2

VLAN Configuration: Select “**Basic**” (Figure E-6)

- Default_1 exists when you use **802.1Q Tag VLAN**.
- Highlight default_1 and click Edit button to add/remove each port.

Tag-based (IEEE 802.1Q) VLAN



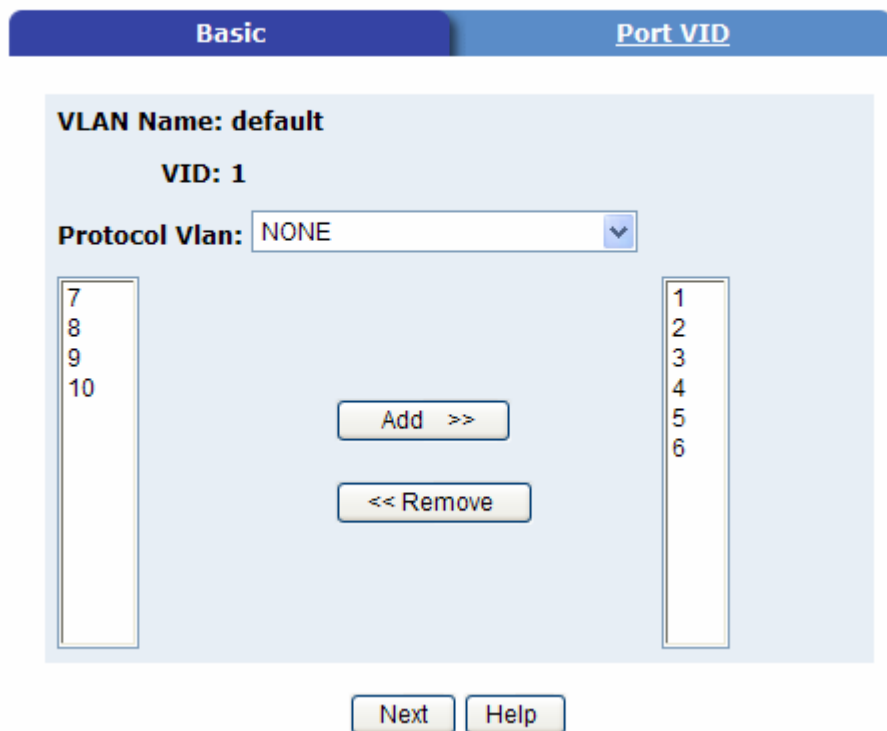
Basic	Port VID	
<p>802.1Q with \without GVRP VLAN Information</p> <table border="1"> <tr> <td>default__1</td> </tr> </table>		default__1
default__1		

Figure E.6 Select “Basic”

In default_1 group, add in or remove group members.

Click Next button to set Tag or Untag for each assigned port. (Figure E-7)

Tag-based (IEEE 802.1Q) VLAN



Basic Port VID

VLAN Name: default

VID: 1

Protocol Vlan: NONE

7
8
9
10

1
2
3
4
5
6

Add >>

<< Remove

Next Help

Figure E.7 Set group members

From this page, you can set Tag or Untag for assigned port and click Apply button. (Figure E-8)

Tag-based (IEEE 802.1Q) VLAN

VLAN Name: default	
VLAN ID: 1	
Port_NO	Setting
1	Untag ▼
2	Untag ▼
3	Untag ▼
4	Untag ▼
5	Tag ▼

Apply

Figure E.8 Set Tag or Untag

Add in new group.

- Click Add button into new group setting page. (Figure E-9)

Tag-based (IEEE 802.1Q) VLAN

Basic
Port VID

802.1Q with \without GVRP VLAN Information

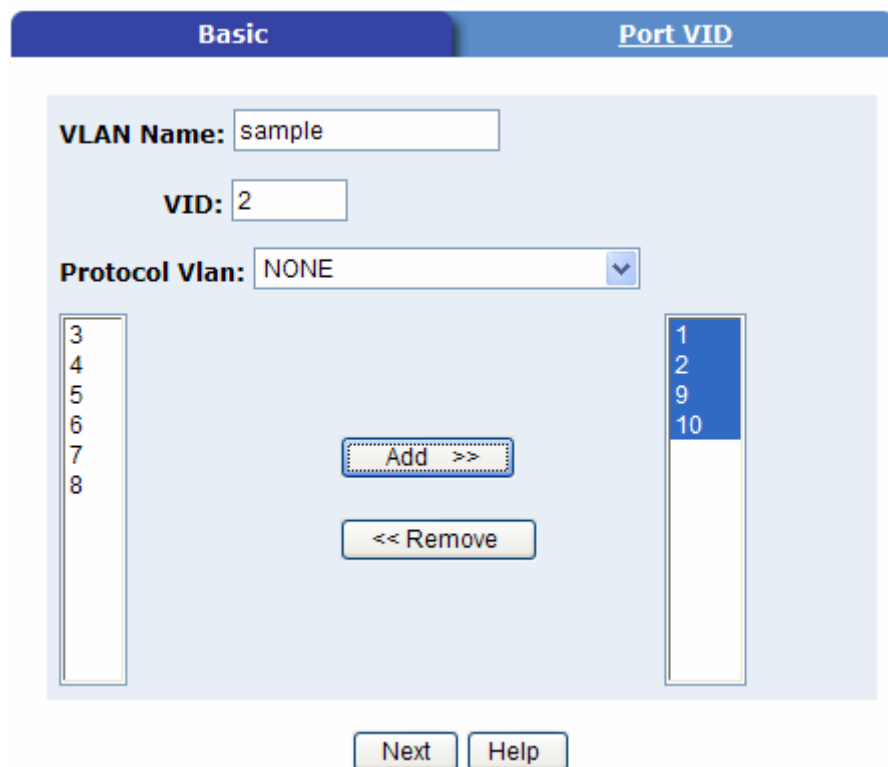
default__ 1

Add
Edit
Delete
PrePage
NextPage
Help

Figure E.9 Add in new group

Add in new group page. (Figure E-10)

- Fill in new group name into VLAN Name.
- Set the VID number.
- Add in new group members.
- Click Next button.



The screenshot shows the 'Add in new group' page with the following details:

- Tabs:** 'Basic' (selected) and 'Port VID'.
- VLAN Name:** sample
- VID:** 2
- Protocol Vlan:** NONE
- Left List (Available):** 3, 4, 5, 6, 7, 8
- Right List (Selected):** 1, 2, 9, 10
- Buttons:** 'Add >>', '<< Remove', 'Next', 'Help'

Figure E.10 Add in new group page

Set Tag or Untag for group members and click Apply button. (Figure E-11)

Tag-based (IEEE 802.1Q) VLAN

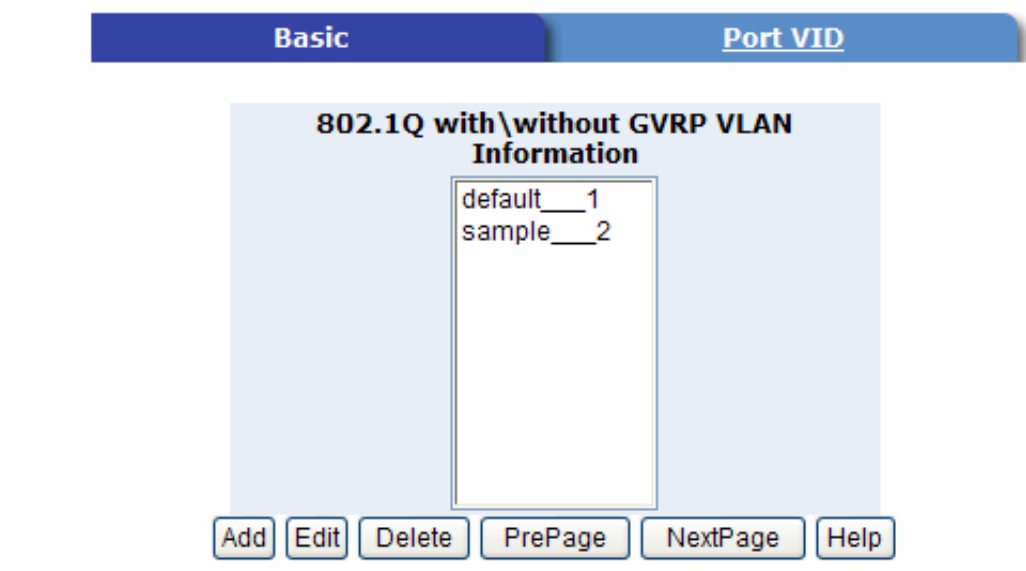
VLAN Name: sample			
VLAN ID: 2			
Port_NO	Setting	Port_NO	Setting
1	Untag ▼	6	N/A
2	Untag ▼	7	N/A
3	N/A	8	N/A
4	N/A	9	Untag ▼
5	N/A	10	Tag ▼

Apply

Figure E.11 Set Tag or Untag

New group has been created, now you can highlight each group and click Edit or Delete button to modify or delete VLAN Group. (Figure E-12)

Tag-based (IEEE 802.1Q) VLAN



Basic Port VID

802.1Q with\without GVRP VLAN Information

default__1
sample__2

Add Edit Delete PrePage NextPage Help

Figure E.12 VLAN group has been created

Appendix F: Compliance and Safety Information

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a computing device, pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. The equipment and the receiver should be connected to outlets on separate circuits.
4. Consult the dealer or an experienced radio/television technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

If this telephone equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance in order for you to make necessary modifications to maintain uninterrupted service.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Important Safety Instructions

Caution1:

The direct plug-in wall transformer serves as the main disconnect for the product. The socket outlet shall be installed near the product and be readily accessible.

Caution2:

Do not use this equipment near water, for example in a wet basement. Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightning.

Caution3:

Do not use the telephone to report a gas leak in the vicinity of the leak.
If trouble is experienced with this unit, please contact customer service of your dealer immediately.

Caution4:

Do not disassemble this equipment. It does not contain any user serviceable components.

FCC Warning

This equipment has been tested to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment can generate, use, and radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at owner's expense.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Warranty

The original owner that the product was delivered in this package will be free from defects in material and workmanship from one year parts after purchase.

There will be a minimal charge to replace consumable components, such as fuses, power transformers, and mechanical cooling devices. The warranty will not apply to any products which have been subjected to any misuse, neglect or accidental damage, or which contain defects which are in any way attributable to improper installation or to alteration or repairs made or performed by any person not under control of the original owner.

The above warranty is in lieu of any other warranty, whether express, implied, or statutory, including but not limited to any warranty of merchantability, fitness for a particular purpose, or any warranty arising out of any proposal, specification, or sample. We shall not be liable for incidental or consequential damages. We neither assume nor authorize any person to assume for it any other liability.

Note: Please do not tear off or remove the warranty sticker as shown, otherwise the warranty will be void.

WARNING
Warranty Void
If Removed

Chinese SJ/T 11364-2006

部件名称	有毒有害物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬[Cr(VI)]	多溴联苯(PBB)	多溴二苯醚(PBDE)
结构壳体	○	○	○	○	○	○
电路组	○	○	○	○	○	○
电源供应器	○	○	○	○	○	○
风扇	○	○	○	○	○	○
线材	○	○	○	○	○	○
包装及配件	○	○	○	○	○	○
<p>○：表示该有毒物质在该部件所有均质材料中的含量均在 SJ/T 11364/2006 标准规定的限量要求以下。</p> <p>×：表示该有毒物质至少在该部件的某均质材料中的含量超出 SJ/T 11364-2006 标准规定的限量要求。</p>						

上述规范仅适用于中国法律